MANUAL DEL REFERENTE

CONECTAR IGUALDAD_

WWW.CONECTARIGUALDAD.GOB.AR

Presidencia de la Nación

ANSES

AUTORIDADES

CRISTINA FERNÁNDEZ DE KIRCHNER
Presidenta de la Nación

JORGE MILTON CAPITANICH
Jefe de Gabinete de Ministros

ALBERTO SILEONI
Ministro de Educación

DIEGO BOSSIO
Director Ejecutivo de ANSES

INTEGRANTES DEL COMITÉ EJECUTIVO

Por ANSES:

DIEGO BOSSIO
Director Ejecutivo de ANSES
Presidente del Comité Ejecutivo

SILVINA GVIRTZ
Directora General Ejecutiva del Programa Conectar Igualdad

Por el Ministerio de Educación de la Nación:

JAIME PERCZYK
Secretario de Educación

Por la Jefatura de Gabinete de Ministros:

SERGIO ANTONIO BLANCO
Subsecretario de Tecnologías de Gestión

Por el Ministerio de Planificación:

LUIS VITULLO
Secretario Ejecutivo del Consejo Asesor del SATVD-T

Abril 2014

ÍNDICE

Procedimiento de Entrega 7
Configuración de routers 8
Servidor Escolar 9
    Configuración Inicial 9
    Cambiar contraseña 10
TSERVER - Servidor de Seguridad 10
Copia de Seguridad - Backup del Servidor 11
Sistema de Seguridad: Tipos de Certificados 13
Configuración Inicial de las Netbooks 15
Certificación de netbooks al servidor escolar 17
Desbloquear una netbook 19
Recuperación de imagen desde las nets 21

ANEXO
Huayra Gestor Escolar 22
Migración Masiva a Huayra 31
    Método 1: Imagen de Restauración 32
    Método 2: Red Cableada con CloneZilla Server 36
Configuración de Access Points: HP V-M200 47
Configuración de Access Points: Micronet 50

PROCEDIMIENTO DE ENTREGA

El **Operador de Logística** acudirá al establecimiento educativo con los equipos para entregar, en la fecha y hora pactada con sus autoridades.
Bajo la supervisión de las autoridades escolares, los alumnos con su DNI accederán a los puestos de entrega donde se verificará que:

a. Figuren en el listado.
b. Figuren en el listado con la marca de "comodato" firmado. De lo contrario, se entregará la netbook a las autoridades escolares bajo firma y aclaración.
c. La autoridad escolar firmará el listado como constancia de recepción en los casos de destinatario con marca de "comodato en proceso".
d. El alumno firmará el listado como constancia de recepción en los casos de destinatarios con marca de comodato firmado y DNI en mano.
e. En los casos de alumnos o alumnas sin DNI, deberán firmar como condición de entrega junto con la Directora o autoridad del Establecimiento Educativo.
f. La caja con la netbook deberá ser abierta en presencia del proveedor del servicio de logística, para verificar el contenido (Netbook + componentes asociados) y el encendido de la computadora.
g. Si se detecta algún tipo de rotura o daño, no encendido o faltante de algún componente, la autoridad escolar deberá dejar constancia del incidente en el Acta de Transferencia que le entregará al proveedor de logística, donde consignará la cantidad de equipos y el n° de serie del equipamiento dañado. Las netbooks deberán ser recibidas y conservadas hasta que se produzca el canje del producto con el correo. Se deberá enviar la imagen del Acta de Transferencia a la Mesa de Servicios del Programa mds@anses.gov.ar, para que se le asigne un número de ticket al reclamo, y se direccione a la Coordinación de Registro y Equipamiento para su seguimiento con el proveedor.
h. El Proveedor del Servicio de Logística deberá obtener la firma de la autoridad escolar en el "Acta de Transferencia" (aprobada por el Comité Ejecutivo del Programa Conectar Igualdad) debidamente conformada.
i. Finalizado el horario de entrega, se pactará con las autoridades del establecimiento una segunda visita para concretar aquellas que quedaran pendientes, por ejemplo, por ausencia de los alumnos.
j. Si luego de esa segunda visita quedaran netbooks sin entregar, se les dará a las autoridades del Establecimiento Educativo la opción de que las reciban bajo su tutela para concretar la entrega en días posteriores. Si el establecimiento educativo no acepta recibir las máquinas remanentes, el Proveedor del Servicio de Logística los remitirá a BUE como "no entregados". Allí se las mantendrá separadas del stock central, debidamente identificadas, y se realizará la rendición al Programa Conectar Igualdad. La información de los equipos rechazados deberá ser cargada en el Aplicativo CONIG INTRA del Programa Conectar Igualdad.
k. Todos los equipos dejados en poder de las autoridades del Establecimiento Educativo seguirán su eventual proceso de entrega y registración a cargo de sus autoridades. Esa situación quedará registrada en el listado de control donde la autoridad escolar deberá firmará por los equipos entregados a su custodia.

CONFIGURACIÓN DE ROUTERS PARA CERTIFICACIÓN DE LAS NETBOOKS

Existen dos opciones de configuración de los routers:

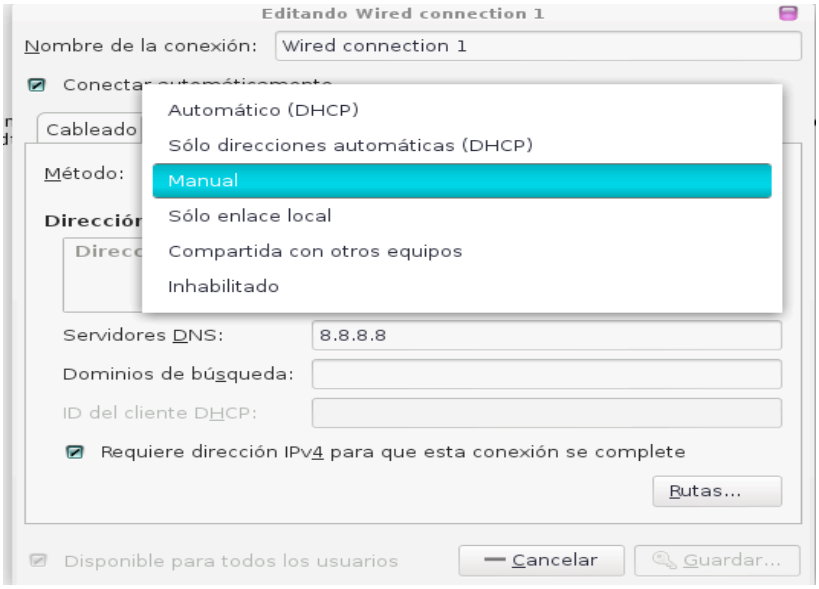
1. Configuración por medio de los script enviados por el equipo de Conectar Igualdad, según los pasos detallados en los Anexos "Configuración de HP / Micronet".
Están disponibles en el escritorio del Huayra Gestor Escolar.

2. Configuración manual:
Para realizar la configuración de los routers debe preverse no hacer los patch como cables cruzados. Ambas salidas (puntas) deben tener la misma norma de colores.
Para poder configurar se necesita:

- 1 Routers Wi-Fi (wireless) Micronet u otro.
- 1 Netbook .
- 2 patch cord o cable de red UTP con fichas RJ45.

Ir al ícono de red y seleccionar **Editar las conexiones**

Una vez ahí nos aparecerá la ventana de configuración de redes.
Seleccionar **Red cableada** --> **Protocolo 4 (TCP/IPV4)**



Añadir: IP: 192.168.2.10 - Máscara de subred: 255.255.255.0 -> Guardar cambios.

Hecho esto, se podrá acceder por medio del navegador a la configuración del router -> 192.168.1.100
El usuario por defecto es ***admin***
Y la contraseña por defecto generalmente es 1234 – puede ocurrir que en las instalaciones de los pisos tecnológicos pueda existir variantes: ***catalina02042009*** o ***CATALINA02042009*** o ***Catalina02042009***

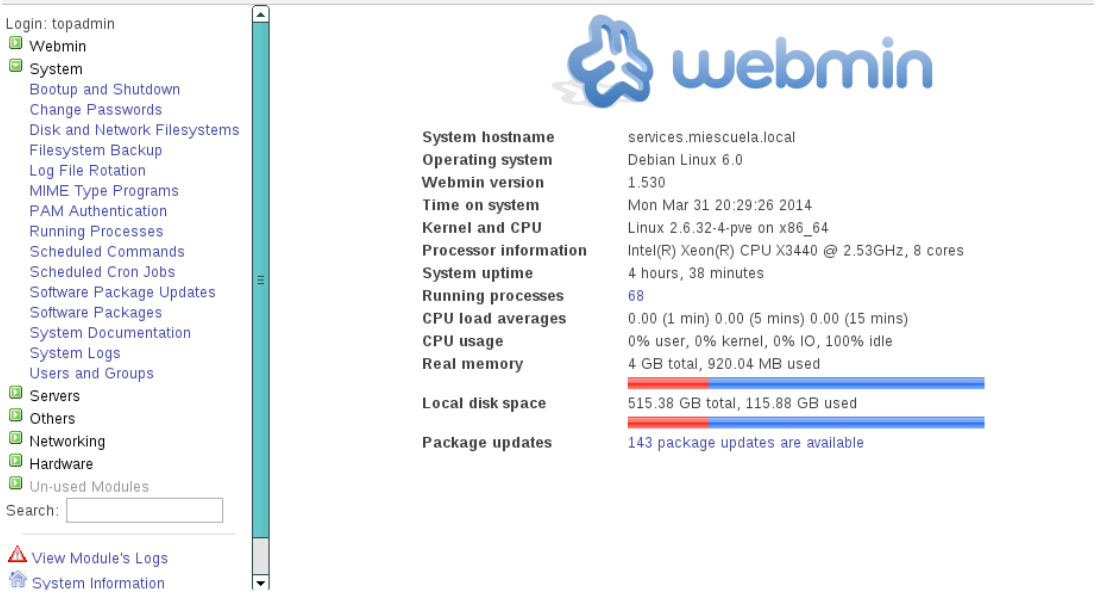
Se podrán especificar las configuraciones que respeten las normas de Conectar Igualdad, y que se necesiten para la certificación y buen uso de la red escolar:

Rango de I.P: 172.16.x.x
Máscara de subred: 255.255.X.X
DHCP Server: deshabilitado.
Modo: AP
Band: 2.4 GHz (G)
MAIN ESSID: "AP 01 – AP1AUla2 – Aula1" (La institución puede normalizar los nombres según lo necesite).

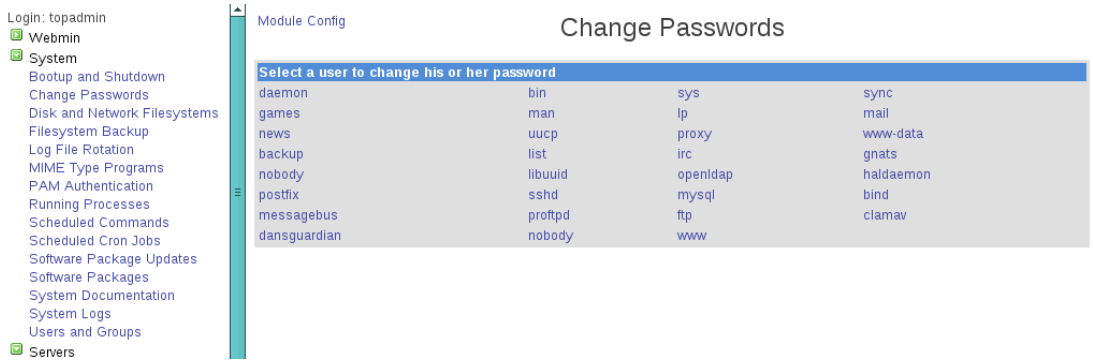
Una vez ingresados los cambios en el AP, guardarlos y modificar la IP ingresada en la net manualmente para la conexión.

SERVIDOR ESCOLAR: CONFIGURACIÓN INICIAL

Para iniciar el trabajo con el servidor, lo primero que se debe hacer es configurar fecha y hora del sistema.
Las contraseñas por defecto del servidor vienen en el Manual del mismo, que se entrega impreso junto al servidor.
Dentro del server abrir una ventana e ingresar
https://localhost:10000



Esto le permitirá el ingreso al Webmin -> ir a Sistema (System) -> Cambiar Contraseña (Change Password) -> elegir el usuario que se quiere editar (admsrv) -> ingresar la nueva contraseña y repetirla.



TDSERVER – SERVIDOR DE SEGURIDAD

Cambiar la contraseña en el TDServer – Servidor de Seguridad
Ingresar al servidor de seguridad: 172.16.0.2/tdserver
Presionar Cambiar contraseña.

Una vez cambiada la contraseña, vuelva a ingresar al TDServer con la nueva contraseña.

Aclaración Importante
Todas las contraseñas correspondientes al Servidor escolar deben ser informadas a la Dirección de la Institución y resguardadas en un formato que corresponda.

COPIA DE SEGURIDAD (BACKUP) DEL SERVIDOR ESCOLAR

Existen dos tipos de copias de seguridad:

1- Copia de Seguridad del Servidor completo (host). Utilizando clonezilla se puede generar.
2- Copia de Seguridad de los servicios del Servidor de Seguridad.

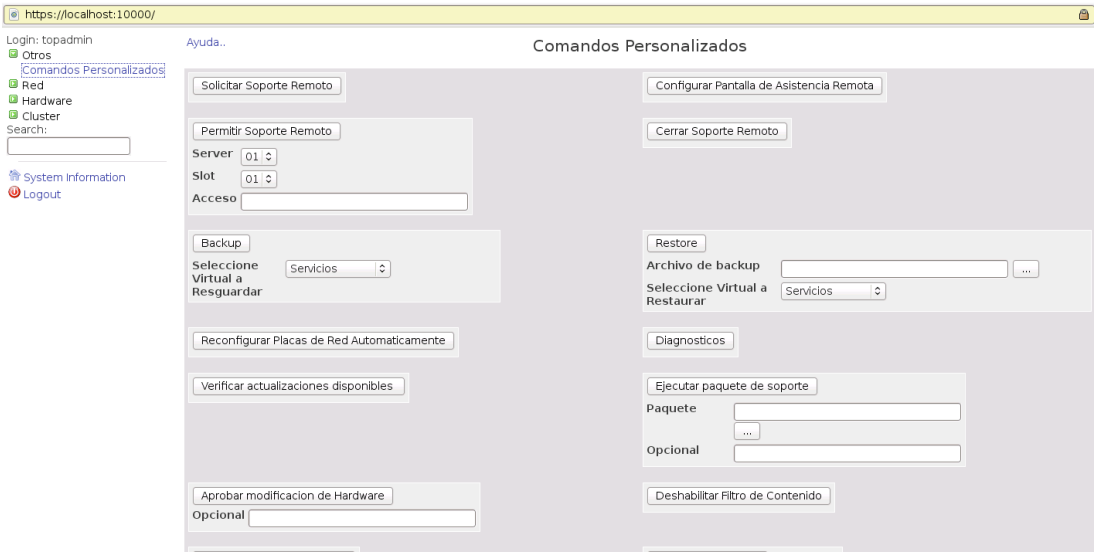
Se recomienda hacer una copia de seguridad cuando se recibe el servidor (esto asegura que la Institución cuente con una copia del servidor entregado desde Conectar Igualdad) y luego, realizar otra cuando se finalice la certificación de todas las máquinas recibidas por primera vez.

1- Copia de seguridad del servidor
Para realizar una copia de seguridad del servidor completo se debe contar con un DVD en blanco para grabar la herramienta que genera la copia de seguridad.
Se debe acceder a home -> topadmin -> soporte -> Imagen Server
* Aclaración: puede llegar a suceder, según la versión del servidor con la que se cuente, que no exista la carpeta "Imagen Server" y la herramienta esté simplemente, alojada en la carpeta soporte.

Una vez dentro se deberá grabar la imagen .iso que existe, para tener la herramienta booteable que genera el backup del host.

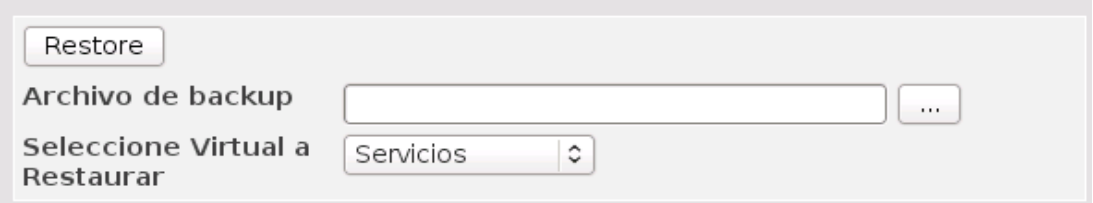
Con la .iso grabada se debe reiniciar y colocar el DVD creado para iniciar desde él.
Al iniciar el encendido del Servidor presione la tecla F10 para visualizar las opciones de booteo. CLONEZILLA LIVE (DEFAULT SETTINGS, VGA 1024X768). Este proceso le solicitará confirmación, por lo que deberá presionar la tecla "y" seguido de la tecla Enter en dos oportunidades. Al finalizar el proceso se abrirá la lectora de DVD, en la pantalla visualizará una leyenda indicando que el proceso ha finalizado correctamente. Le pedirá que retire el DVD de la lectora y reinicie el Servidor.
El archivo será alojado en la carpeta Soporte, dentro de la Carpeta Personal.

2- Copia de seguridad de los servicios del servidor.
Para realizar las copias de seguridad de las máquinas virtuales que trae el servidor se debe: Ingresar al navegador del servidor -> 172.16.0.1:1000 -> Otros -> Comandos personalizados



Dentro de la pantalla aparecerá la opción de hacer los backups de las máquinas virtuales. Seleccionar la máquina virtual: TDServer (hace la copia de seguridad del Servidor de Seguridad de Conectar Igualdad). Servicios (copia los servicios virtuales que posea el servidor), Usuarios (copia los usuarios creados y administrados dentro del webmin).

Estos backups se encuentran dentro de la carpeta Soporte -> Backups.
Para restaurar los backups solamente se debe acceder nuevamente al Servidor Host y seleccionar Otros -> Comandos personalizados -> Restaurar o Restore.



Aclaración Importante

En los servidores Ubuntu, no existe la virtualización de servicios, por lo cual se debe realizar el backup completo del host (explicado en el Paso 1), teniendo en cuenta que el backup será de todo lo que posea el servidor exceptuando lo que se posea en /var/share.

Por lo cual se debe tener en cuenta que las copias de backups hechos que están dentro de la carpeta soporte, si no son extraídos del servidor, pueden llegar a incrementar el peso que tenga la imagen final del backup realizado.

Se recomienda realizar una Copia de Seguridad cada vez que exista algún cambio importante dentro de las máquinas virtuales que requiera ser resguardado. Por ejemplo en la certificación de máquinas, o renovación de certificados.
Y siempre entregar los mismos a la Dirección de la Institución, para que en caso de surgir una necesidad se cuente con el material.

SISTEMA DE SEGURIDAD
TIPOS DE CERTIFICADOS

CERTIFICADO DE ARRANQUE COMÚN

Este certificado funciona como certificado regular de las netbooks asociadas al servidor. Es otorgado por el servidor, cada vez que la netbook entra en riesgo (según la fecha de expiración y según la cantidad de arranques).

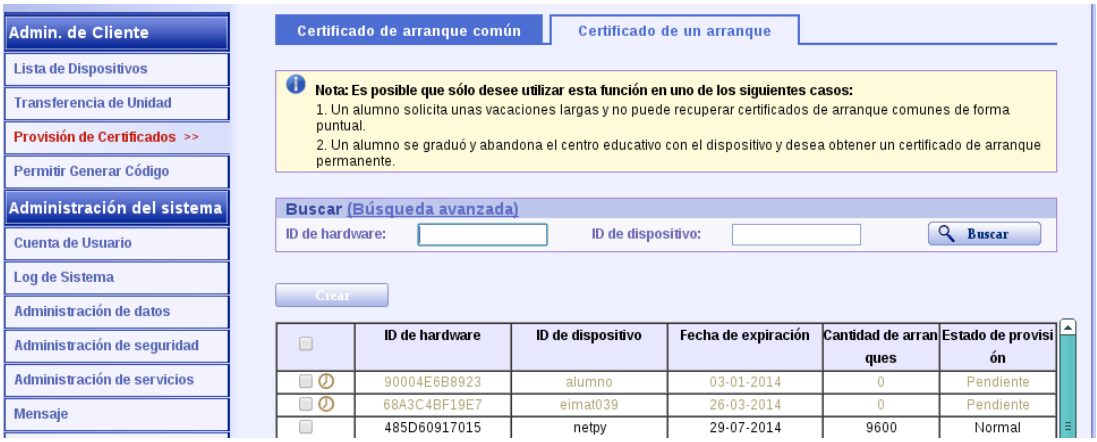
Se debe detallar:

· Duración de expiración del certificado de arranque: cantidad de días que tendrá el certificado. Aquí se debe tener en cuenta, en los períodos de receso, que la cantidad de días no sea menor a los días de receso, para evitar el bloqueo de máquinas en esos días.

· Número estimado de inicios por día: cantidad de arranques que pueda tener la netbook en el día.

· Número total de arranques: el total de arranques restantes que tendrá la netbook.

CERTIFICADO DE UN ARRANQUE



Este certificado se entrega con fecha específica. Para entregarlo, se debe buscar por ID de hardware o ID de dispositivo.
Generalmente el uso de este certificado es para dar una fecha específica de vencimiento por condiciones especiales, por ejemplo: un alumno que tiene licencia por enfermedad.
Aclaración: la cantidad de arranques viene predeterminada por defecto, según lo establecido en el certificado de arranque común.

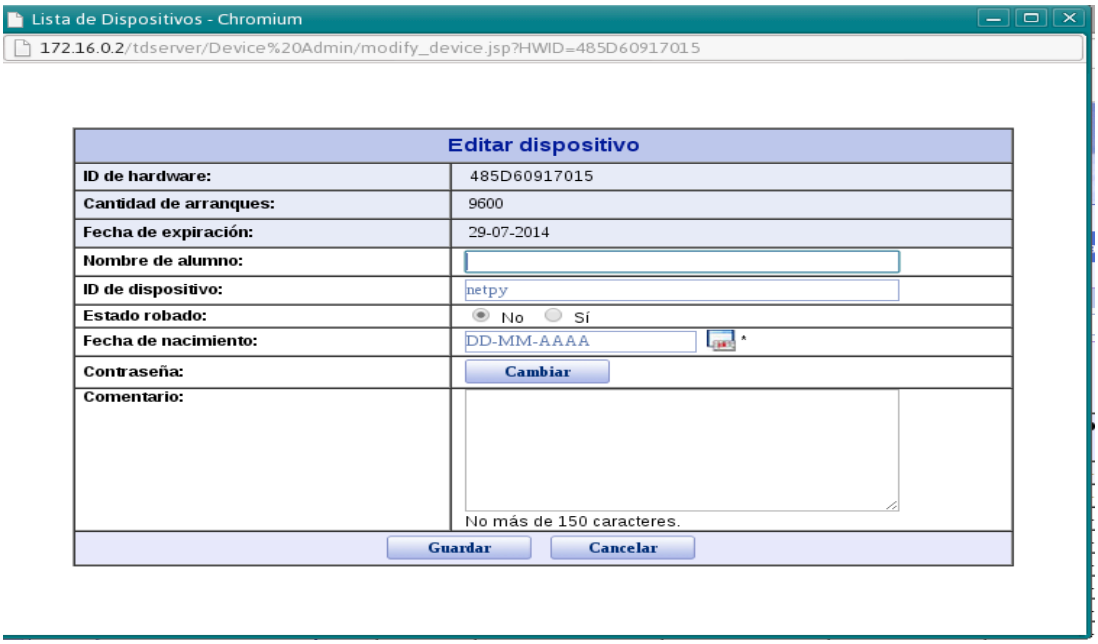
CERTIFICADO PERMANENTE

El certificado permanente se entrega a alumnos egresados de la Institución una vez que hayan aprobado todas las materias del último año, dentro del ciclo lectivo.
La forma de configurarlo es igual a la de Certificado de un Arranque.

MÁQUINA ROBADA

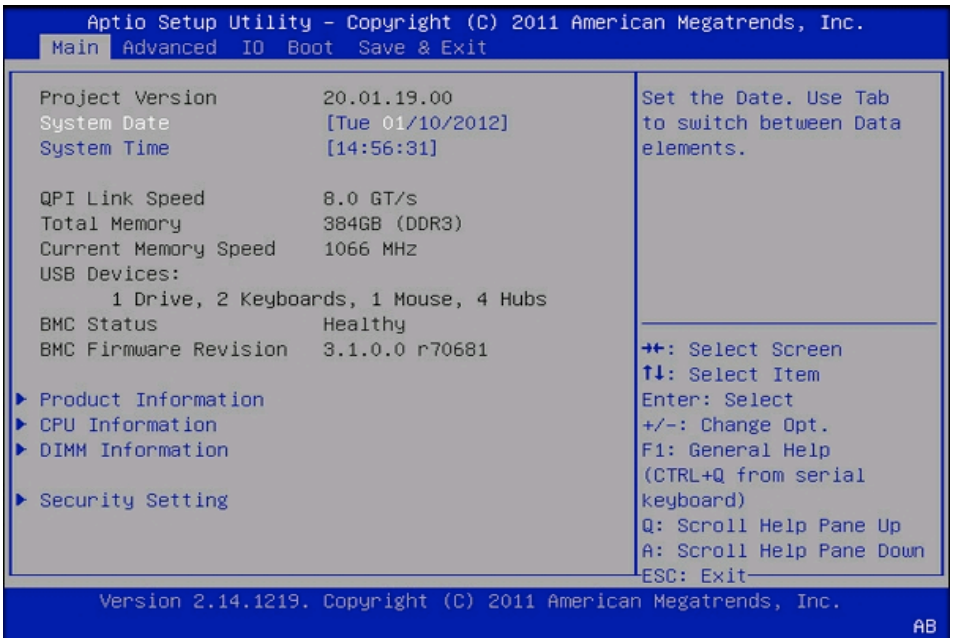
Cuando sucede un ilícito o un alumno deja de ser alumno regular de la escuela, y es necesario bloquear la máquina. Se debe marcar esa máquina dentro del TDServer a fin de que cuando se conecte a la red escolar, cambie el estado de certificación. Para esto, se debe buscar en Listado de Dispositivo por ID de Hardware o ID de Dispostivo -> presionar

sobre el ID de Hardware y aparecerá el cuadro de edición de datos de la netbook.
Se debe seleccionar el “Estado robado” - **SI.**
Una vez hecho esto se deben guardar los cambios ralizados y cuando el dispositivo se conecte a la red escolar cambiará su estado.



CONFIGURACIÓN INICIAL DE LAS NETBOOKS

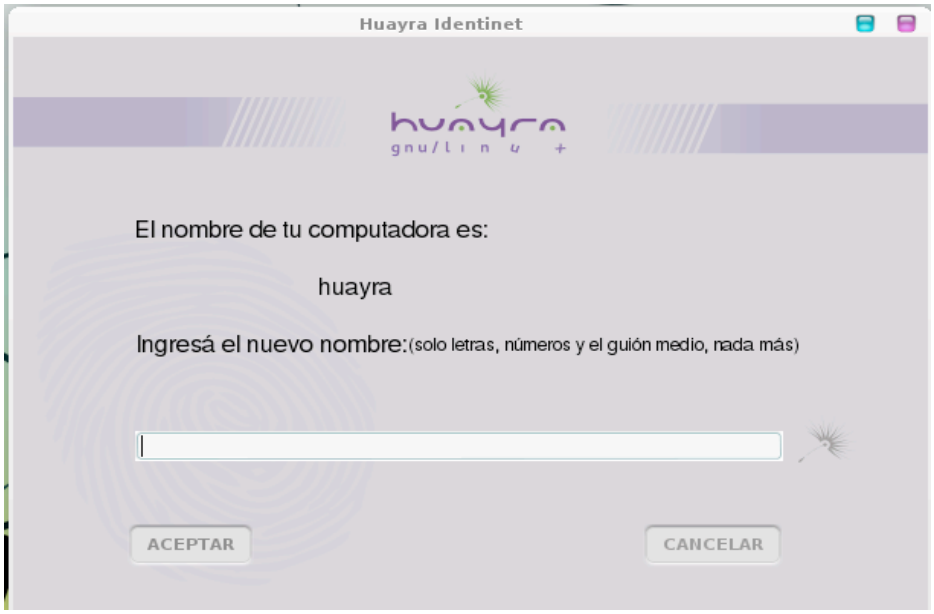
Para modificar los parámetros de fecha y hora de las netbooks se debe ingresar al iniciar en el BIOS presionando SUPR
– Modificar el IDIOMA, en caso de que Español no figure.
– Establecer Fecha y Hora correspondiente.



F10 para guardar los cambios

CAMBIAR EL NOMBRE DEL EQUIPO

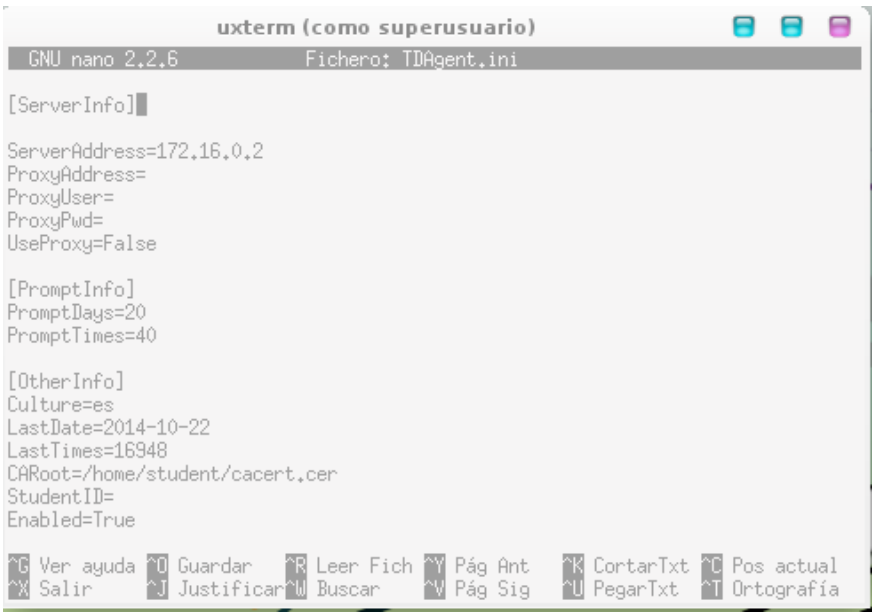
En Huayra ingresar al Menú de Aplicaciones -> Huayra -> Huayra Identinet
Dentro del Identinet permitirá cambiar el nombre del equipo.



MODIFICAR EL AGENTE PARA LA CERTIFICACIÓN DE LA NETBOOK

Edición del archivo

En Huayra se debe abrir la terminal de root -> escribir “cd etc/thefdeterrent” -> una vez estemos dentro de la carpeta thefdeterrent -> escribir “nano TDAgent.ini” -> desplazarse por los parámetros a editar y modificar los valores correspondientes:
ServerAddress= “” -> “172.16.0.2”
Heartbeat_Interval=”10” -> “1”
PromptDay= “20”



Una vez modificado presionar Ctrl + X -> “S” -> presionar Enter -> “S”

En Windows se encuentra dentro del Disco C -> Archivos de Programas (Program Files) -> Intel Learning Series -> Thef Deterrent -> AgentConfig.ini
Se lo puede editar con el block de notas.

Una vez editado el archivo, se debe reiniciar la máquina.

Conectarse a la red inalámbrica que corresponde al servidor para realizar la certificación

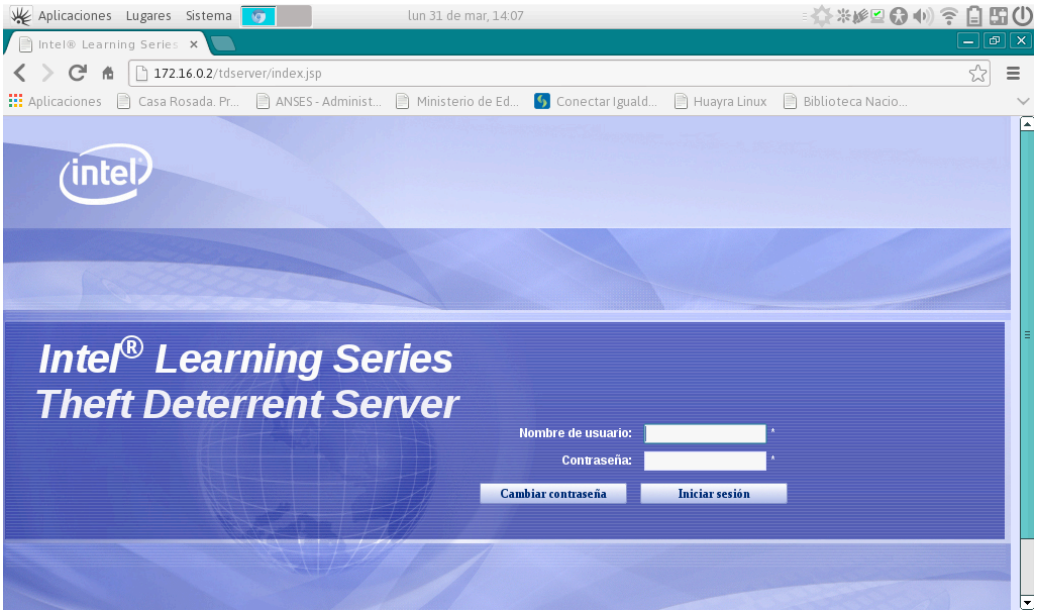
CERTIFICACIÓN DE LAS NETBOOKS AL SERVIDOR ESCOLAR

Las netbooks vienen preasociadas al servidor de la escuela y se debe terminar el proceso de certificación una vez que estén en las escuelas.

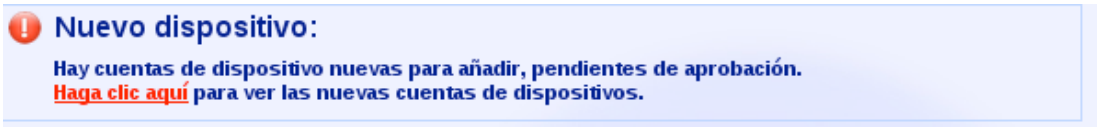
Para esto:
En la netbook
En Huayra una vez configurado el archivo TDAgent.ini y conectado a la red inalámbrica del servidor escolar, aparecerá el ícono del Agente en rojo.

Al hacer doble click sobre el mismo podrá verse si la dirección en el mismo corresponde al servidor: 172.16.0.2
Una vez ahí se debe ir a aprobar la netbook desde el TDServer

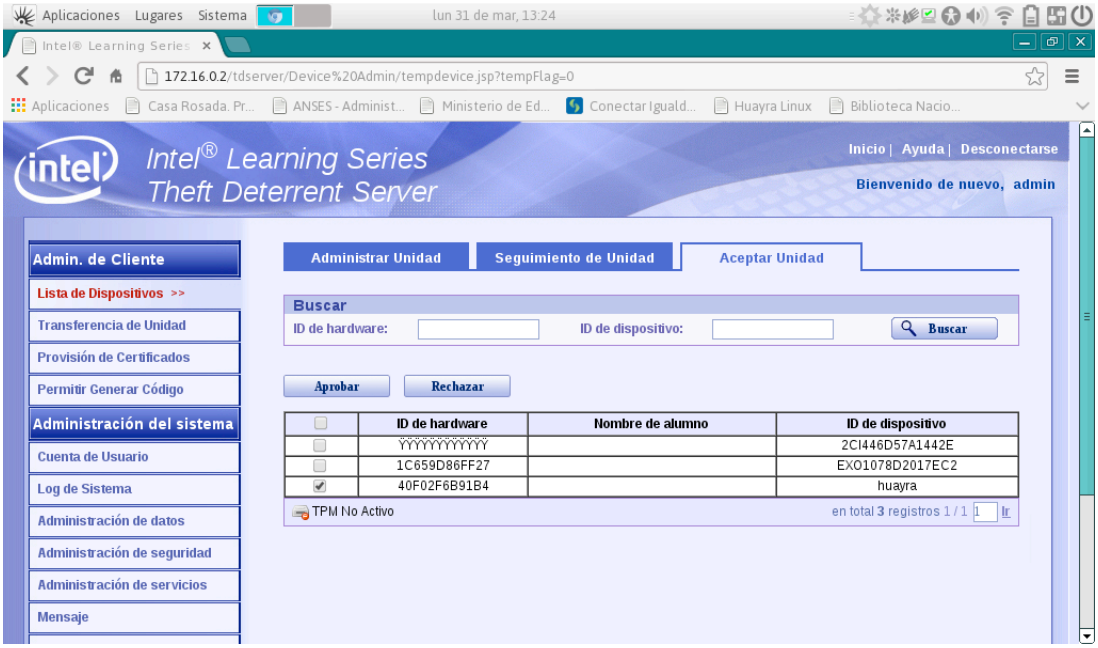
En el servidor
Ingresar al TDServer. 172.16.02



Se debe ingresar el usuario y la contraseña que se definió para el TDServer
Una vez ahí, si la netbook no fue aprobada antes en el servidor, figurará un cartel de “Nuevos dispositivos para Aprobar”



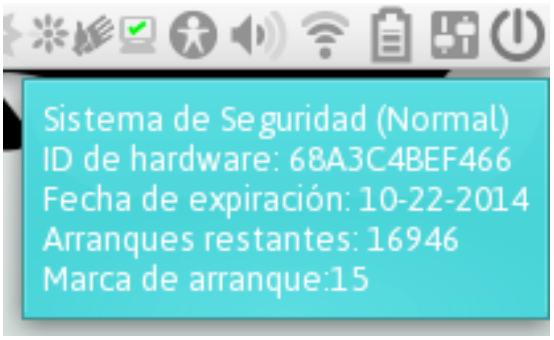
Haciendo click allí, figurarán las netbooks que están conectadas a la red del servidor y que no fueron aprobadas.



Si los datos que muestran son los correctos (ID de hardware, ID de dispositivo) seleccionar la máquina y darle Aprobar.
La netbook tardará unos minutos en tomar el certificado y mostrará un aviso de reinicio. Puede llegar a necesitar dos reinicios hasta tomar el certificado con la fecha configurada por el referente.

Aclaración: según el sistema operativo en el que se certifique, sucede que el Agente queda directamente en verde, mostrando la fecha configurada correctamente sin necesitar reiniciar la máquina.

Una vez que haya finalizado el proceso de certificación el ícono del Agente dentro de la netbook quedará en verde, y al posicionarse sobre él, mostrará la cantidad de arranques restantes y la fecha de expiración.

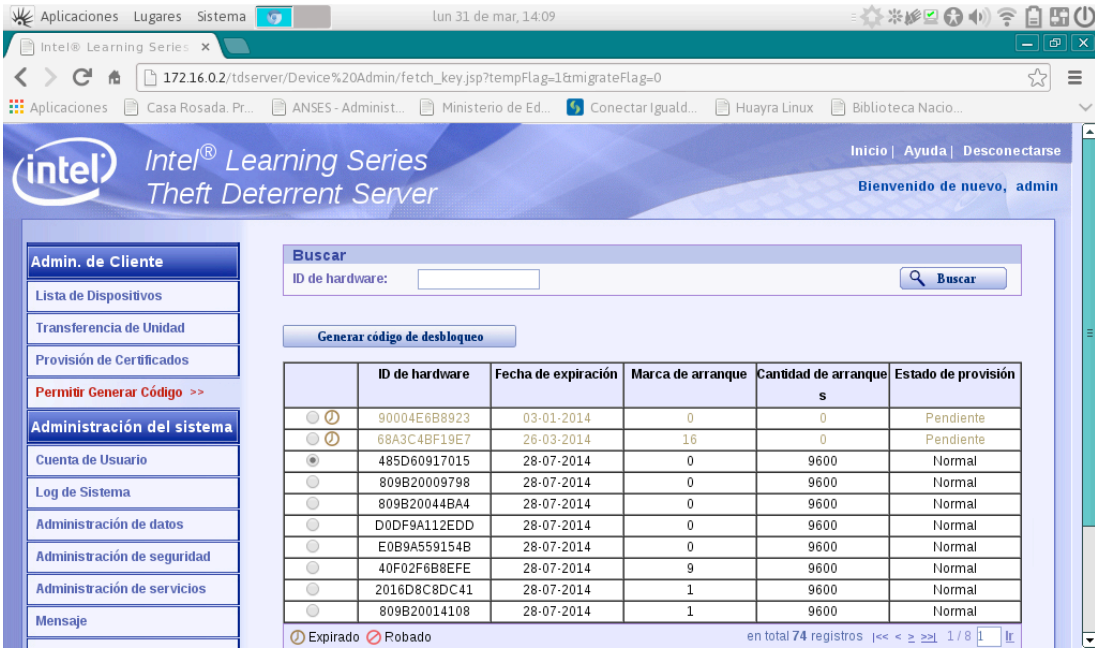


DESBLOQUEAR UNA NETBOOK

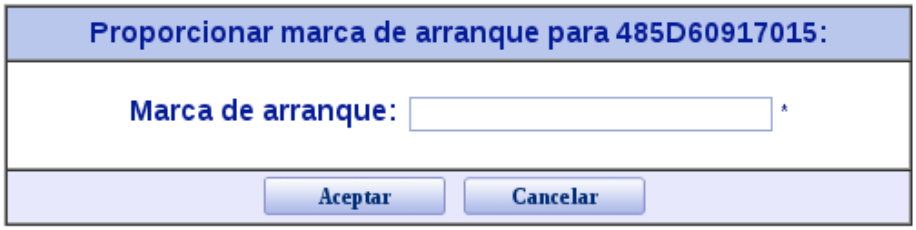
Si la netbook ya fue enlazada y viene bloqueada (porque superó la cantidad de arranques o superó la fecha de expiración) se debe generar un Código de Desbloqueo desde el TDServer.

Para esto es necesario:
– Que la netbook figure dentro del listado de dispositivos aprobados en el Servidor.
– Obtener el Hardware Id.
– Obtener la Marca de Arranque o Boot Tick.

Ingresar al TDServer
En el menú elegir la opción “Permitir Generar Código”

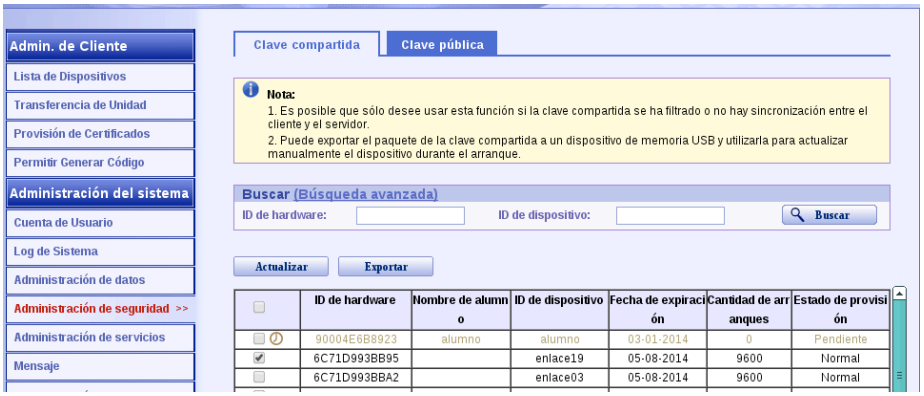


Buscar por id de hardware la netbook -> Click en Generar Código de desbloqueo -> colocar el número de Marca de Arranque o boot tick que figure en la netbook.



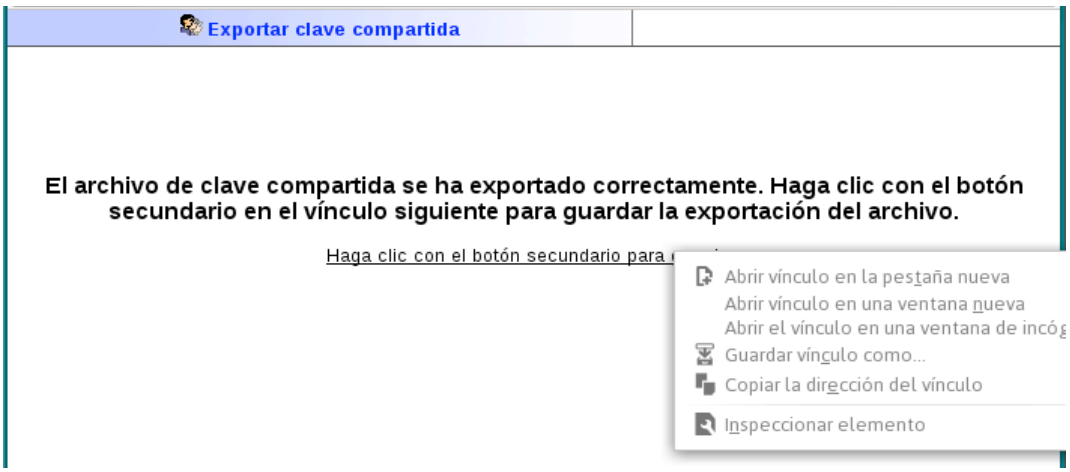
Una vez hecho ese paso, se le dará un código de 10 dígitos para desbloquear la máquina.
Luego de desbloquear la net ingresará al sistema operativo y tendrá 9 arranques restantes.
Para ingresar al sistema operativo se debe conectar a la red que corresponde al servidor y esperar que tome el certificado de arranque común (según lo configurado por el referente).

---- En caso de que la netbook haya sido asociada al servidor, pero no permita desbloquearla lo que se puede hacer es sincronizar las llaves públicas manualmente, para comprobar que tengan las mismas.
Para esto dentro del TDServer, se debe acceder -> Administración de Seguridad -> buscar la netbook por ID de Hardware o ID de dispositivo -> seleccionar la netbook y click en exportar.



Una vez allí se debe guardar el archivo “tcopp.bin”. - “Guardar vínculo como”
Aclaración: se debe colocar ese archivo en un dispositivo portable que tenga formato “FAT 32 o fat16” a fin de que permita luego levantarlo desde la netbook bloqueada.

Una vez hecho esto, se debe colocar el dispositivo en la netbook bloqueada.
Presionado las teclas Ctrl + Insert debe mostrar un cartel con letras verdes como el siguiente:



Dará 10 arranques para permitir realizar la actualización de certificado correspondiente.

Aclaración importante
Este proceso de sincronización de llaves, también se realiza cuando existe un cambio de escuela o una nueva asociación de máquinas por medio de paquetes de provisión.

RECUPERACIÓN DE IMAGEN DESDE LAS NETS

Existen dos posibilidades de recuperación de la imagen de cada net.
La primera es hacerlo mediante una herramienta de clonación como puede ser el clonezilla o el ghost. Seguir los pasos en el Anexo adjunto "Migración Masiva"

La segunda es hacerlo mediante la recuperación de cada sistema operativo, por ejemplo. Dentro de la imagen grub (la siguiente captura) de la netbook aparecerá la opción de restaurar sistema.

Cabe aclarar, que la restauración del sistema se hace siempre sobre el sistema operativo que corresponde, dejando sin modificar los datos que estén guardados dentro del disco "Datos" de las netbooks.

HUAYRA
GESTOR ESCOLAR

En esta guía veremos paso a paso cómo utilizar el Gestor Escolar de Huayra.

Lo primero que nos vamos a encontrar es con la caja que envía el Correo Argentino. Dentro de la caja nos vamos a encontrar con el kit de Huayra Gestor escolar que está compuesto por los siguientes materiales:

-1 Netbook con Gestor Escolar Huayra.
-1 Access Point (AP) marca HP modelo V-M200
-1 Access Point (AP) marca Micronet

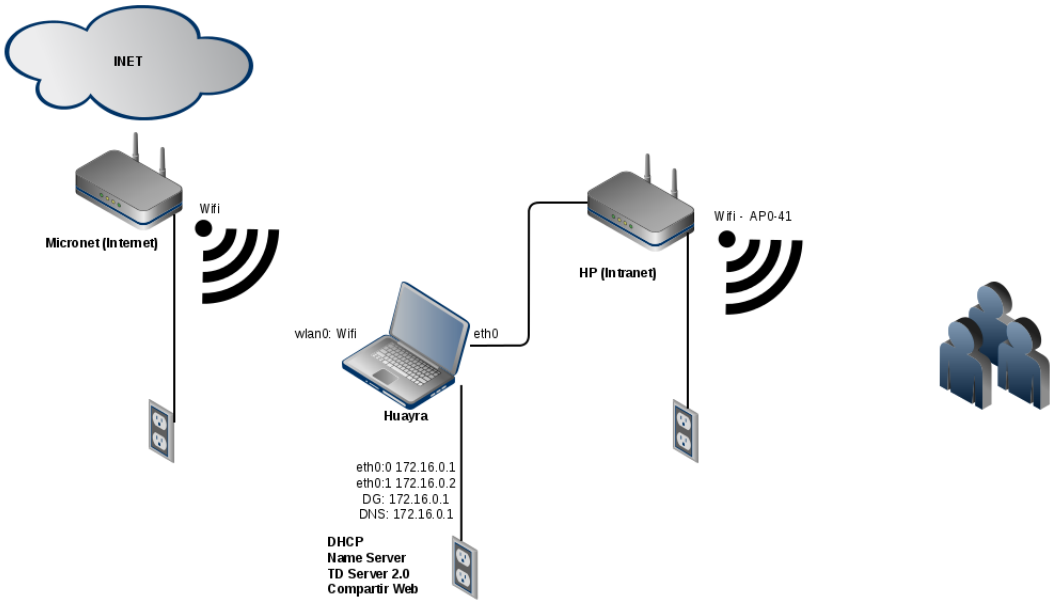
¡SE RECOMIENDA LEER LA GUÍA ANTES DE REALIZAR CUALQUIER CONEXIÓN !

PASO 1 - GUÍA DE CONEXIÓN DE LOS AP AL GESTOR ESCOLAR HUAYRA

En primer lugar conectaremos la red interna que brindará conectividad entre el **Gestor** y las **netbooks**. Para tal fin, conectamos el AP marca HP por medio del cable de red provisto a la placa LAN del Gestor Escolar.

Dependiendo el modelo la boca de red puede variar la ubicación, puede estar al costado izquierdo como derecho.

Entonces nuestros equipos deberían quedar así dispuestos, como en la imagen a continuación.



CONEXIÓN A INTERNET:

De disponer de una conexión a internet en la escuela utilizaremos el AP marca Micronet. Este AP se envía pre configurado para la mayoría de los proveedores de internet, en caso que su conexión requiera autenticación, deberá configurar la misma bajo las especificaciones del prestador.

En el Gestor la conexión a esta red, se encuentra preestablecida por lo cual cuando esté disponible, la conexión se realizara en forma automática.

En caso de no conectar automáticamente, se puede hacer en forma manual, dando clic en el icono de conexiones Activas, en la barra de inicio y ahí seleccionar “Conig”.

¿SE PERDIÓ LA CONFIGURACIÓN DEL AP?

Si por alguna razón se ha perdido la configuración de los AP no se preocupe, puede entrar a la carpeta que se llama “Documentos para administrador” ubicada en el escritorio. Dónde se guarda la información necesaria para volver a configurar los AP.
Si lo que falla es el AP que provee la conexión a internet, vea entonces la carpeta Micronet.
Si lo que falla es el AP que provee de conectividad a la red escolar interna, entonces vea la carpeta de HP.

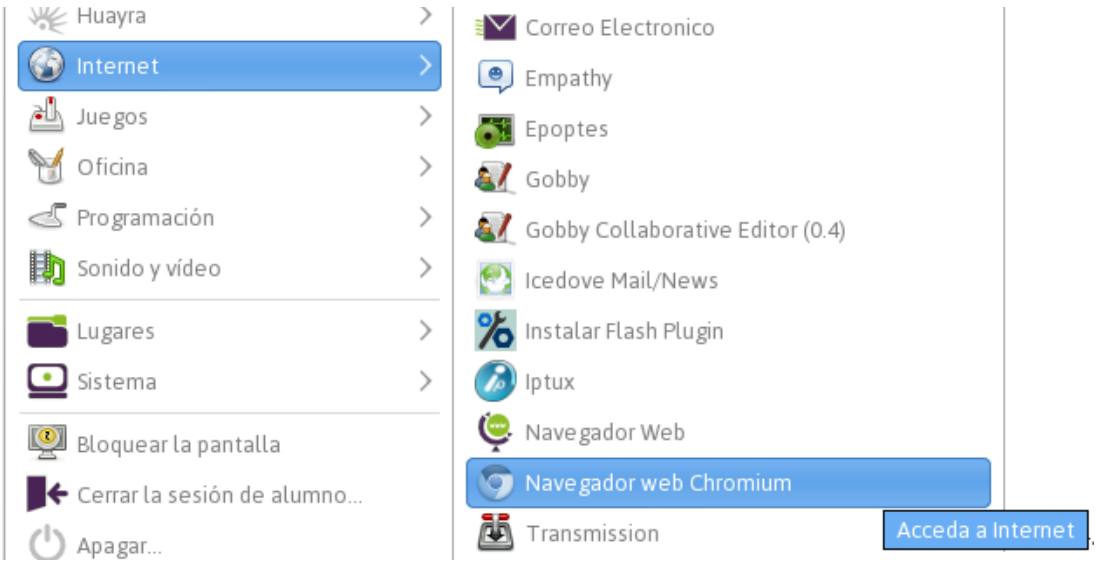
PASO 2 - INICIO DE SESIÓN INICIAL

Una vez que tenemos todo conectado, ahora vamos a proceder a encender el **Gestor Escolar Huayra**. Lo primero que nos va a solicitar es que ingresemos el nombre de usuario y contraseña.

Usuario del Gestor Escolar Huayra: **huayra-admin**
Contraseña: **huayra-admin**

PASO 3 - ACCESO AL TDSERVER

Para acceder al TDS debemos abrir un navegador web, para eso vamos al ícono del panadero ubicado en la esquina superior izquierda de la Netbook.

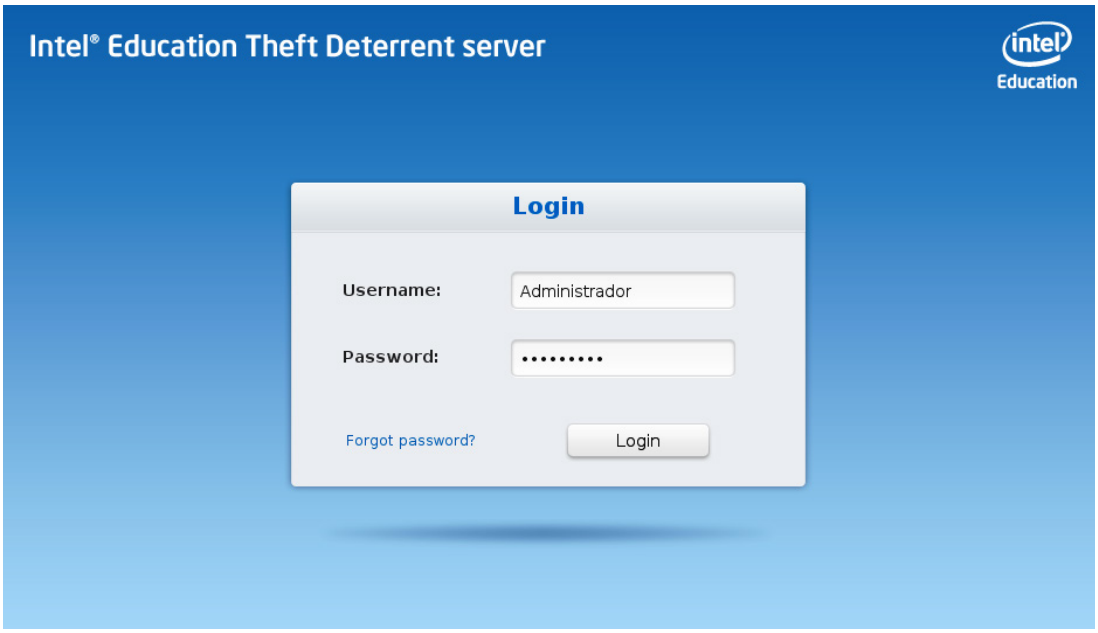


Una vez que abrimos nuestro navegador, vamos a ingresar:

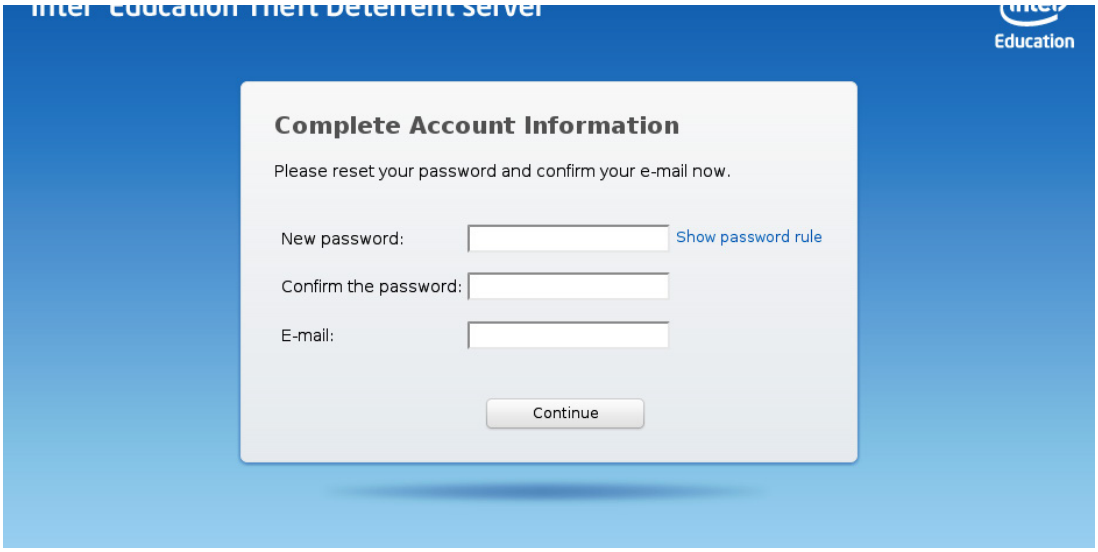
https://172.16.0.2 o **https://tdserver**

¡IMPORTANTE: PARA EVITAR INCONVENIENTES AL MOMENTO DE INICIAR SESIÓN, SE DEBE RESPETAR MAYÚSCULAS, MINÚSCULAS Y SIGNOS DE PUNTUACIÓN.!

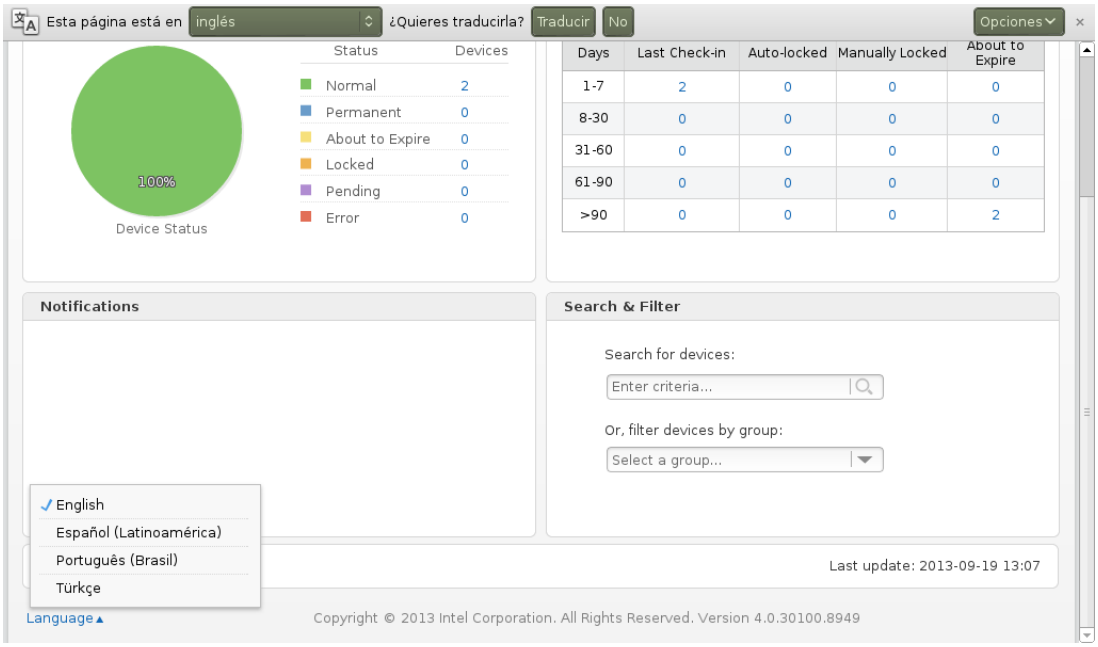
PASO 4 - INTRODUCCIÓN AL THEFT DETERRENT SERVER (TDS)



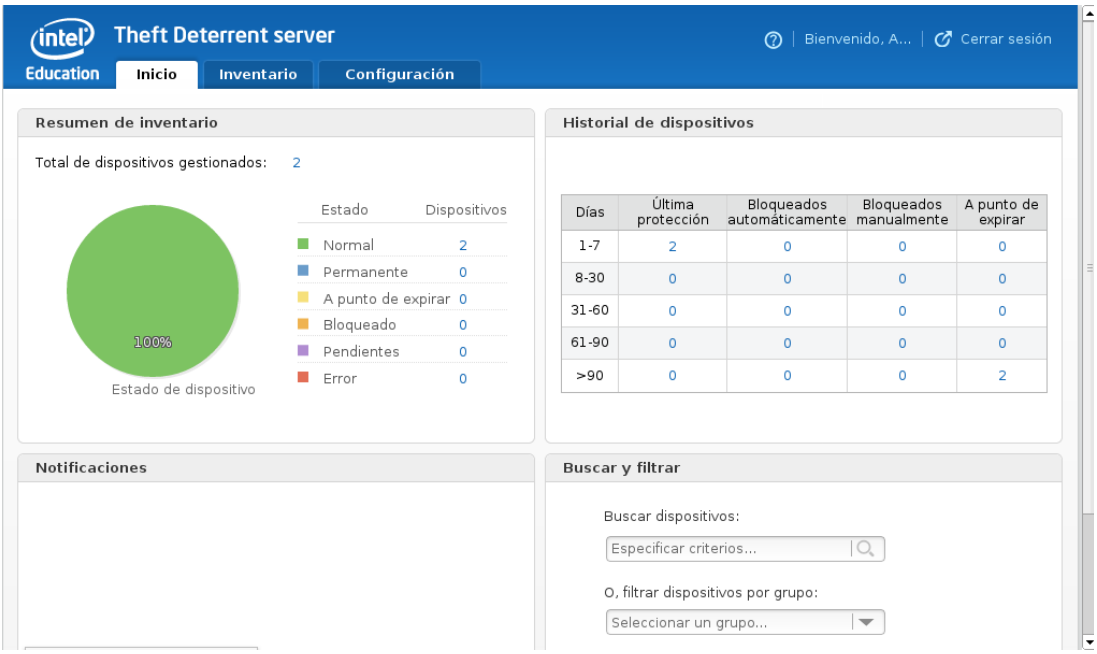
Una vez iniciada la sesión el programa nos pedirá que cambiemos la contraseña.



Al iniciar por primera vez al TD server, este lo hace en idioma inglés por defecto. Para modificarlo en la parte inferior izquierda, se encuentra la opción “Language”, donde seleccionaremos “Español (Latinoamérica)”.



PESTAÑA INICIO



RESUMEN DE INVENTARIO

Presenta en un gráfico circular, los estados de los dispositivos conectados al TDS. Los estados pueden ser:

- Normal: dispositivos enlazados al TDS.
- Permanente: dispositivos con un certificado permanente, siendo este el caso de los estudiantes egresados del establecimiento.
- A punto de expirar: dispositivos a punto de bloquearse.
- Bloqueados: dispositivos que se encuentran bloqueados.
- Pendientes: dispositivos pendientes de aprobación.
- Error: dispositivos que no tomaron certificados. Esto puede ser causa de un pro blema con el chip tpm, o un error de comunicación entre la red y el dispositivo.

HISTORIAL DE DISPOSITIVOS

Los números de la tabla representa el número de dispositivos que fueron certificados, bloqueados auto y manualmente

NOTIFICACIONES

Las notificaciones que se visualizan permiten ver cuando se produzcan determinados eventos:

	Error: Existe un conflicto dentro del TDS
	Atención: Notificaciones sobre el estado de provisión de los dispositivos (equipos a punto de bloquearse, existencia de equipos pendientes de aprobación, etc.)
	Información: Notificaciones generales sobre los dispositivos

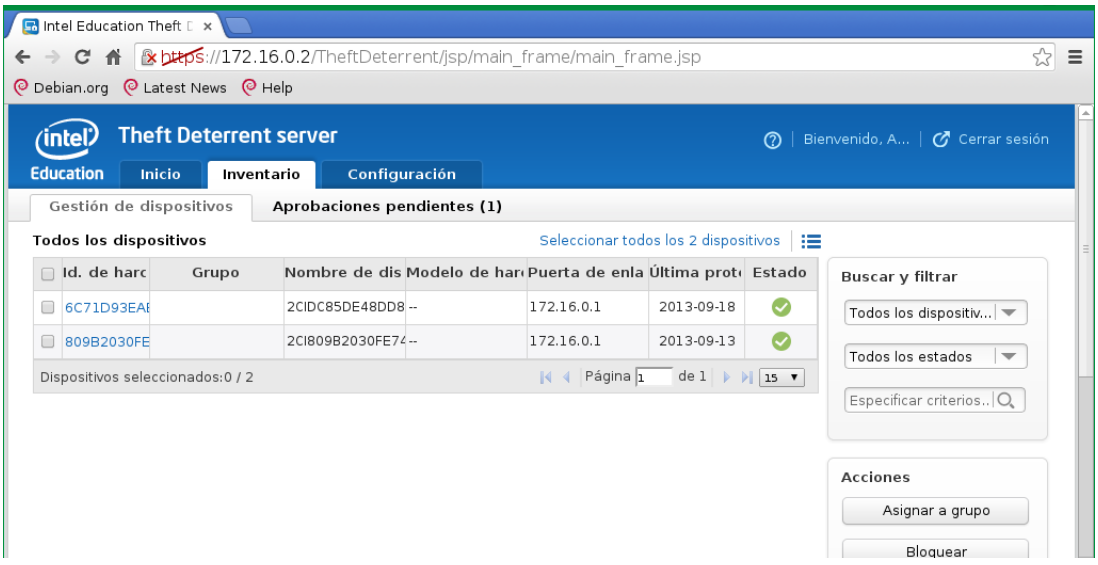
¿QUÉ HAGO SI EN EL TDS TENGO UN DISPOSITIVO PENDIENTE DE APROBACIÓN QUE NO PERTENECE A NINGUNO DE LOS ESTUDIANTES O DOCENTES?

Es importante identificar el usuario del dispositivo. Podría ser el caso de docentes que realizan actividades en otros establecimientos educativos que cuenten con el Programa Conectar Igualdad y que sus dispositivos se encuentren enlazados en otro servidor.
En estos casos, es recomendable utilizar la opción “Rechazar dispositivo” dentro la pestaña “Aprobaciones pendientes” en “Inventario”.

INVENTARIO

GESTIÓN DE DISPOSITIVOS

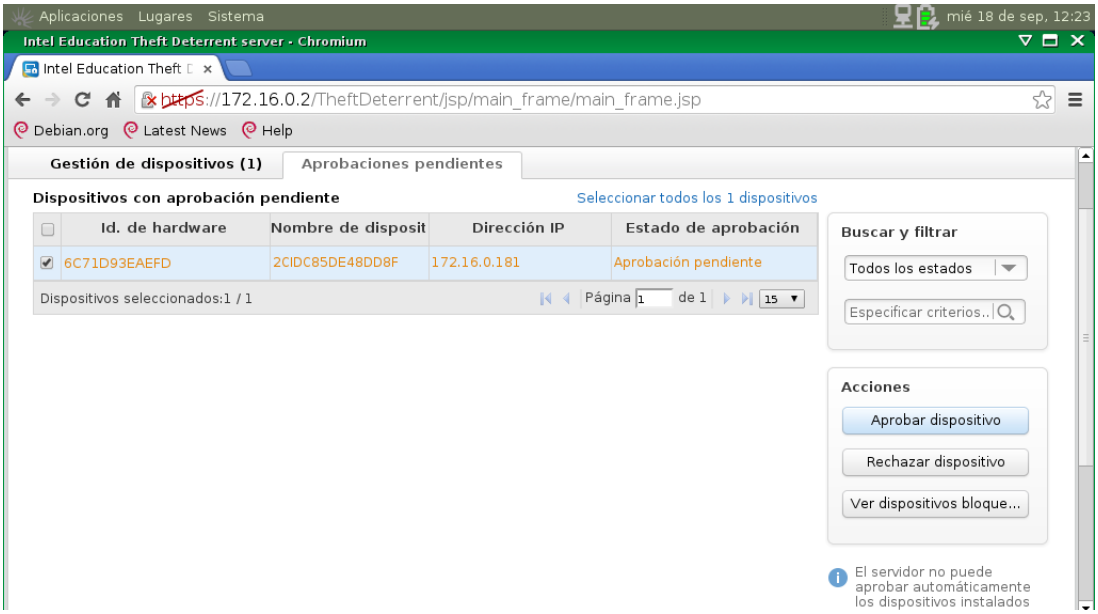
Lista todos los dispositivos que se encuentran enlazados al TDS. Desde aquí, se podrá bloquear manualmente, desbloquear, aprovisionar un nuevo certificado de arranque único, etc.



APROBACIONES PENDIENTES

Lista todos los dispositivos que se encuentran pendientes de aprobación para ser ingresados en el TDS. Desde aquí, se podrá aceptar o rechazar dispositivos nuevos.

Los dispositivos se encuentran identificados mediante el **ID DE HARDWARE** del dispositivo.



APROBACIÓN DE DISPOSITIVOS

Para enlazar dispositivos nuevos al TDS es **necesario** conectarlos a la red escolar. De manera predeterminada, se conectarán automáticamente a la red mediante el "Ap01".

Desde el TDS, en la pestaña "Aprobaciones pendientes", ubicada bajo "Inventario", se listarán todos los dispositivos conectados a la red escolar que ya se encuentran habilitados para ser enlazados. En caso de que el listado esté incompleto, refrescar la página presionando la tecla F5.

1. Ingresar a "Inventario"
2. Seleccionar la pestaña "Aprobaciones pendientes"
3. En el listado de dispositivos con aprobación pendiente, seleccionar mediante la casilla de verificación (ubicada a la izquierda de la columna de Id. de hardware) los dispositivos que se desean ingresar. Esto se puede realizar de manera individual (seleccionando de a uno) o seleccionando todos los dispositivos listados mediante la casilla de verificación ubicada en la parte superior izquierda de la tabla.

4. Una vez seleccionados los dispositivos, hacer clic en la acción "Aprobar dispositivo"
5. Al aprobar el dispositivo, el estado de aprobación cambiará a "Esperando protección", y en un margen de tiempo de veinte minutos, el dispositivo descargará el certificado, el cual debe ser aceptado
6. Desde el dispositivo a ingresar, elegimos la opción "Sí", y esto nos solicitará reiniciar.
7. Una vez reiniciado el dispositivo, el mismo estará provisionado y en el TDS figurará en el listado de Gestión dispositivos, en donde figurará con el ícono de Estado normal.

IMPORTANTE:

En caso de que sea necesario rechazar un dispositivo:

1. Ingresar a Inventario
2. Seleccionar la solapa Aprobaciones pendientes
3. Seleccionar el dispositivo a rechazar, haciendo clic en la casilla de verificación
4. Clic en la acción "Rechazar dispositivo"

En caso de haber rechazado un dispositivo erróneamente:

1. Ingresar a Inventario
2. Seleccionar la solapa Aprobaciones pendientes
3. Seleccionar la acción "Ver dispositivos bloqueados".
4. En el listado de dispositivos bloqueados, seleccionar la casilla de verificación del dispositivo que queremos recuperar
5. Clic en la acción "Quitar"

De esa manera, se sacará de la lista de bloqueados para volver a aparecer como pendiente.

BLOQUEO Y DESBLOQUEO DE DISPOSITIVOS

En casos en donde se requiere la no renovación de certificados (dispositivos robados, extraviados, etc.), se puede bloquear manualmente.

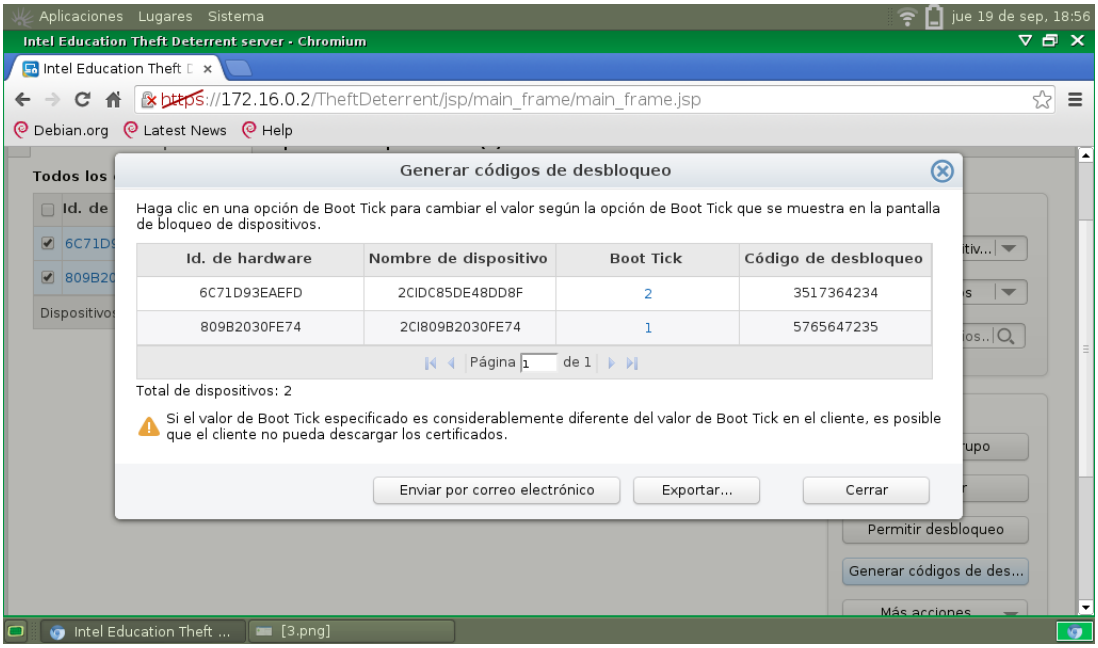
Una vez seleccionado el dispositivo, se debe realizar clic en la acción "Bloquear". Allí aparecerá la opción de ingresar un comentario, donde se podrá describir el caso para futura referencia.

Importante: Este proceso se puede revertir. En el caso de que el dispositivo se haya recuperado, se debe seleccionar y hacer clic en la acción "permitir desbloqueo".

GENERACIÓN DE CÓDIGO DE DESBLOQUEO

Para desbloquear un dispositivo que cuenta con un certificado expirado, se deben seguir estos pasos:

1. Ingresar a Inventario
2. Seleccionar la pestaña Gestión de dispositivos
3. Seleccionar la casilla de verificación de el/los dispositivos a desbloquear
4. Clic en la acción "Generar código de desbloqueo"



5. Ingresar el código en el dispositivo bloqueado. Si se ingresó correctamente, el dispositivo debería desbloquearse inmediatamente. Cómo el dispositivo contará con solamente diez arranques, es importante que, una vez conectado el dispositivo a la red escolar, verificar que se haya descargado el certificado nuevo.

APROVISIONAR NUEVO CERTIFICADO

¿Cuándo se emiten los certificados especiales?:

- Un estudiante tiene que faltar por una enfermedad o
- Porque ya egresó (certificado permanente).
- Alguna otra razón que la escuela considere necesaria.

Se puede aprovisionar un nuevo certificado temporal o permanente. Los certificados permanentes se emiten en los dispositivos para los estudiantes que hayan egresado y cumplan la normativa vigente.

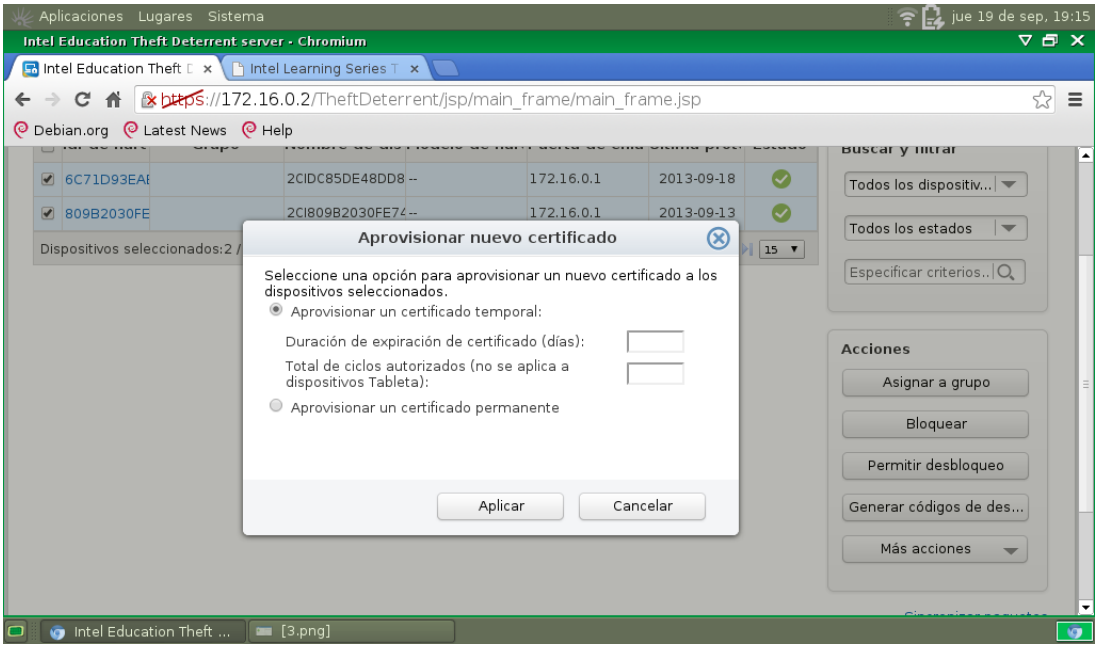
Los certificados temporales se emiten en los siguientes casos:

- Receso escolar
- Ausencia prolongada de un docente o estudiante

Para emitir un nuevo certificado, realizar los siguientes pasos:

1. Ingresar a Inventario
2. Seleccionar la pestaña Gestión de dispositivos
3. Seleccionar los dispositivos a provisionar
4. Clic en “Más acciones…”
5. Seleccionar la acción “Aprovisionar nuevo certificado”

Se abrirá una ventana donde se podrá especificar la duración (en días) y los ciclos de certificado (arranques del dispositivo). También se podrán emitir certificados permanentes. Una vez completada la información requerida, haciendo clic en “Aplicar”, el TDS emitirá los nuevos certificados a los dispositivos seleccionados previamente.



Nota: Se recomienda que durante el receso escolar, aprovisionar los dispositivos con un certificado no menor a noventa días y setecientos arranques.

MIGRACIÓM MASIVA A HUAYRA

En este tutorial vamos a ver cómo hacer una migración de varias netbooks a Huayra, reemplazando la versión de Linux que ya estaba instalada. Estos métodos permiten, replicar la imagen de Huayra que se encuentra en una netbook madre a varias netbooks.

¡IMPORTANTE!
PARA HACER UNA MIGRACIÓN MASIVA ES NECESARIO QUE TODAS LAS NETBOOKS QUE SE VAN A MIGRAR TENGAN LA MISMA ESTRUCTURA DE PARTICIONES EN EL DISCO RÍGIDO, LOS MISMOS NOMBRES, TAMAÑOS Y UBICACIÓN QUE LA NETBOOK MADRE

PASO 0: INSTALAR LA ÚLTIMA VERSIÓN DE HUAYRA EN UNA NETBOOK

Existen **2 métodos** principales de migración masiva: por imagen de restauración y por multicast con un servidor CloneZilla. En este tutorial vamos a explicar ambos, pero antes para poder realizar cualquiera de ellos es necesario tener una netbook con la última versión de Huayra instalada.

Para ello tenés que seguir los siguientes pasos

Requerimientos
Imagen ISO de Huayra estable.
Pendrive de al menos 4 gigas.
Netbook con doble partición.

PASO 1

Instalar en el pendrive la última imagen estable de Huayra según los pasos explicados en el manual de Generar Pendrive booteable.

PASO 2

Iniciar Huayra LIVE y seguir los pasos de instalación recomendados aquí, reemplazando la partición de Linux anterior.

PASO 3

Una vez instalado Huayra, realizar una imagen de la partición de Huayra usando CloneZilla.

MÉTODO 1:
IMAGEN DE RESTAURACIÓN

Requerimientos

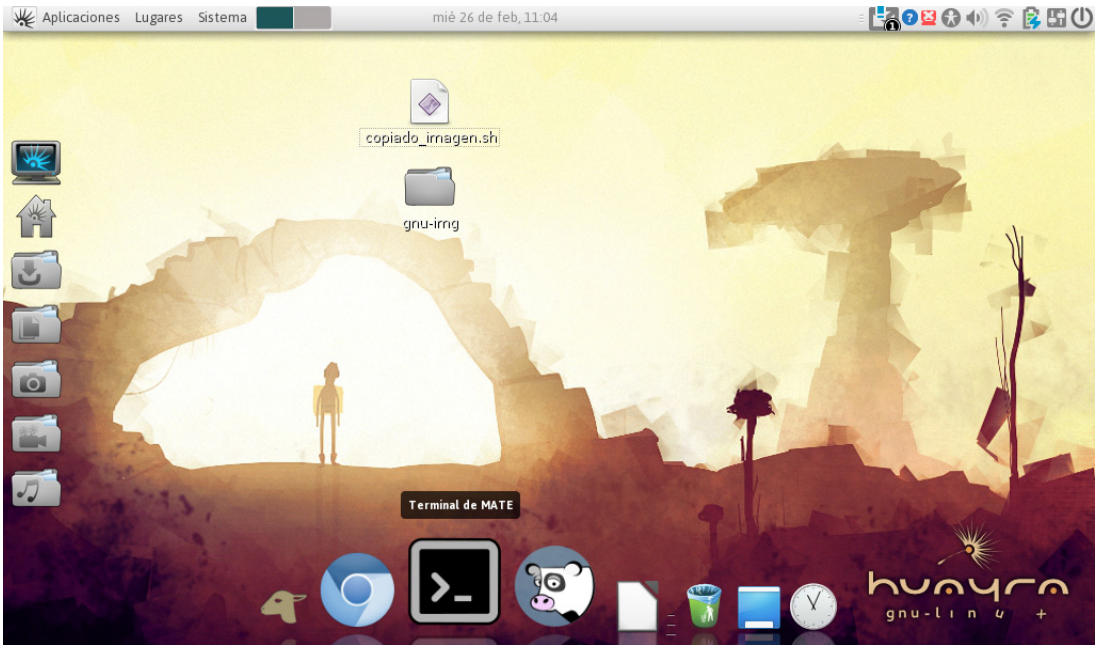
· Imagen hecha con CloneZilla de la partición de Huayra en un dispositivo extraíble (existen numerosos tutoriales sobre como utilizar CloneZilla para crear esta imagen).

· Tener el script que reemplaza la imagen de recuperación que ya existe en la netbook con una imagen que incluya Huayra. Este script se encuentra para descargar desde el sitio de Huayra (http://huayra.conectarigualdad.gob.ar).

Mediante este método se puede utilizar una imagen de Huayra hecha con CloneZilla para reemplazar la imagen de restauración existente (siempre y cuando las netbooks tengan la misma estructura de particiones en el disco). Una vez hecho esto se hace una restauración del equipo.

PASO 1

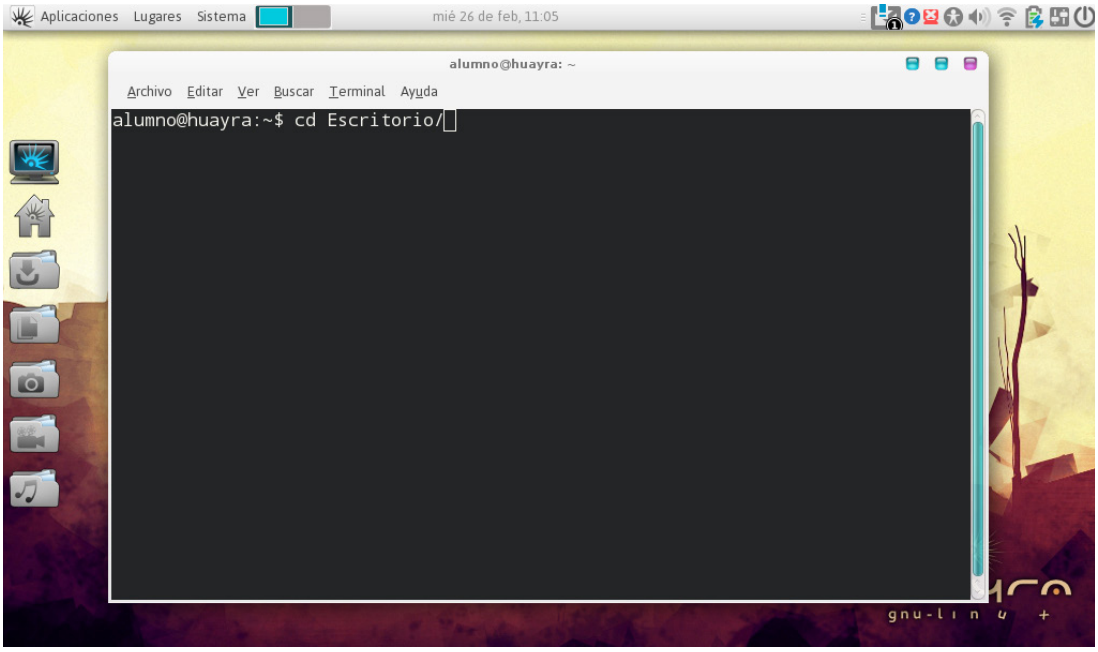
Copiar la imagen hecha con el CloneZilla** de la partición de Huayra y el script (de copiado) en un directorio común (por ej.: el Escritorio) de la máquina en la cual se va a sobreescribir la partición de recuperación.



**Importante. La carpeta que contiene la imagen generada por CloneZilla tiene que llamarse gnu-img.

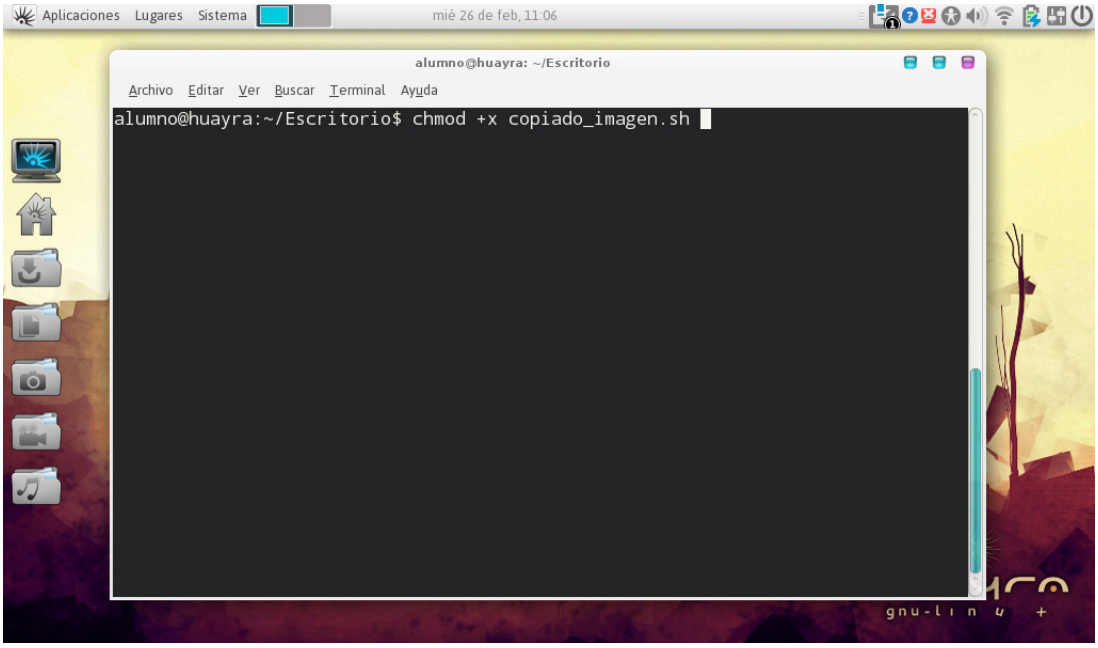
PASO 2

Para poder utilizar el script hay que hacerlo ejecutable.
Abrir una terminal de comandos y posicionarse en el directorio donde se copiaron el script y la imagen (en el ejemplo **/home/Escritorio**)



PASO 3

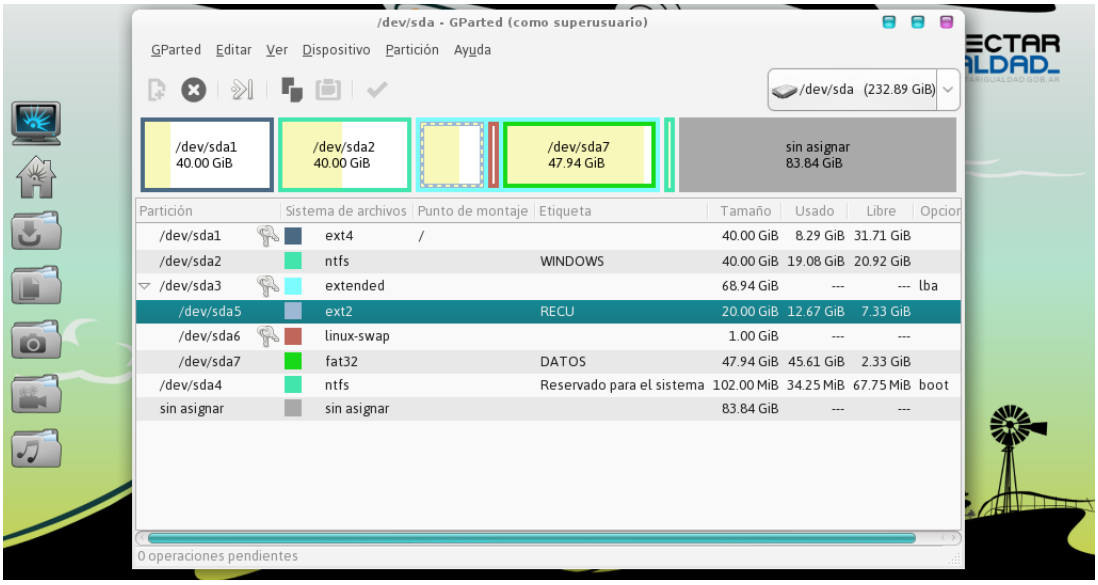
Ingresar al directorio en el cual se encuentra el archivo y con el comando **chmod +x nombre_del_script** convertirlo en ejecutable (en el ejemplo **sudo chmod +x scriptcopiado**).



PASO 4

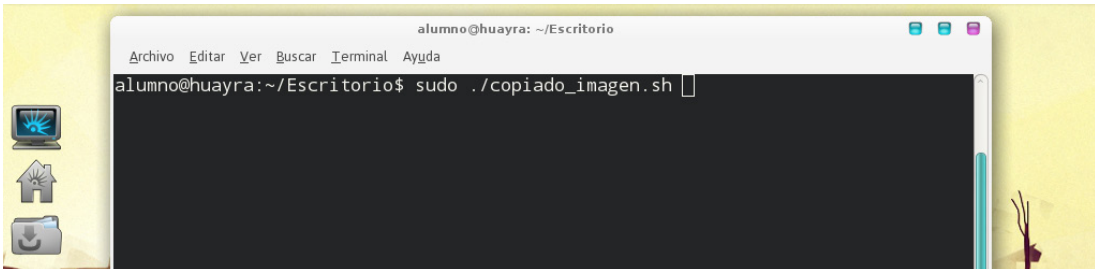
El paso siguiente va a ser ejecutar el script que reemplaza la imagen de restauración con la nueva imagen que contiene Huayra. Para esto el script de copiado va a preguntar cuál es el número de la partición de recuperación en la máquina. Si no lo sabe puede utilizar el programa **GParted** (en **Sistema -> Administracion -> GParted**) para saber cual es su número.

En la imagen de ejemplo la opción es **sda5**

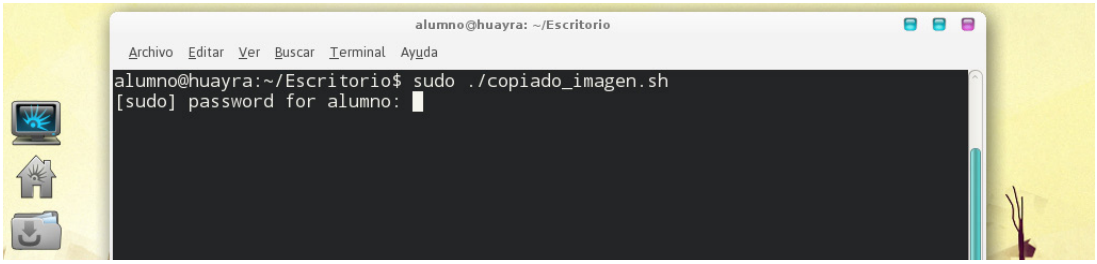


Paso 5

Ejecutar el script con el comando **sudo ./copiado_imagen.sh**

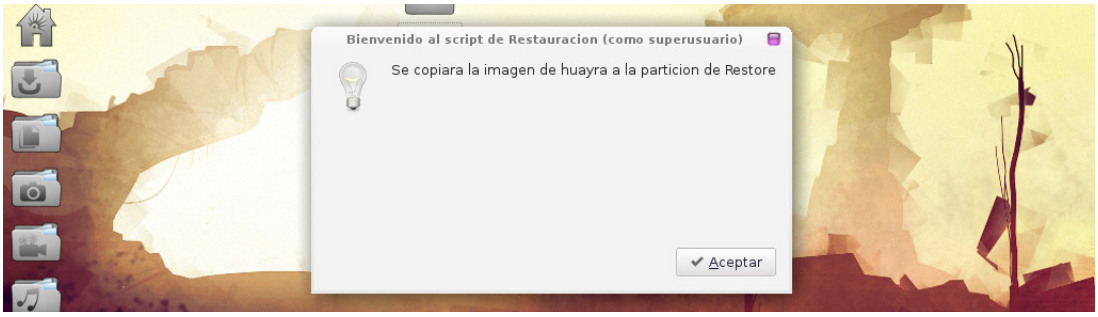


Ingresar la contraseña con permisos de administrador



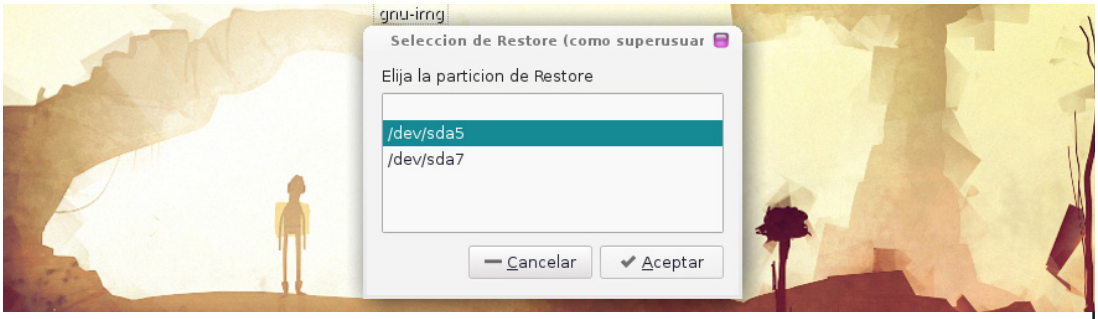
Paso 6

El script informa que se encuentra reemplazando la imagen de restauración. Hacer clic en **Aceptar**



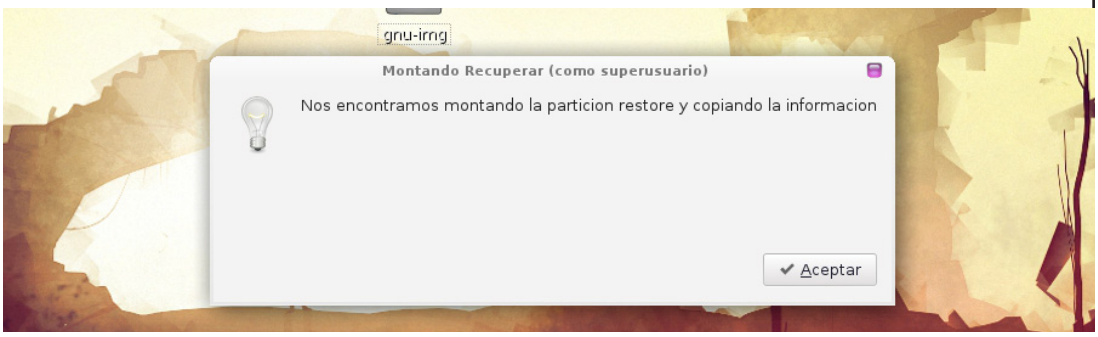
Paso 7

Elegir la partición de restauración en función de lo visto en el Paso 4



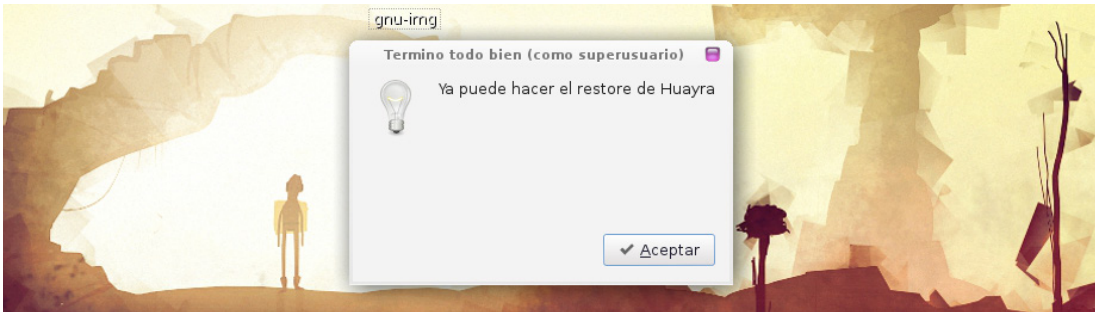
Paso 8

El script informa que se encuentra montando la imagen de restauración. Hacer clic en **Aceptar**



Paso 9

Se terminó de reemplazar la imagen. Hacer clic en Aceptar



Paso 10

Reiniciar la netbook y en el grub seleccionar la opción que posee el numero de partición seleccionado en el script como partición de recuperación (generalmente sda5 o sda7).

Dejar que se cargue el método de recuperación y luego volver a reiniciar la netbook para asegurarse que inicie correctamente.

MÉTODO 2:
RED CABLEADA CON CLONEZILLA SERVER

Requerimientos

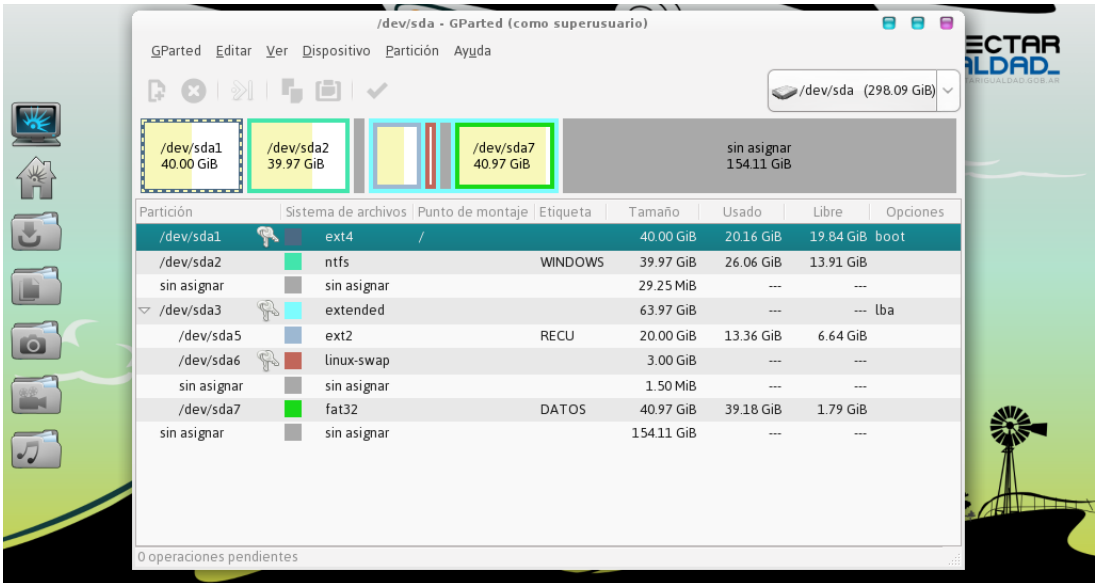
· Imagen hecha con CloneZilla de la partición que contiene Huayra actualizado y la partición de recuperación en un dispositivo extraíble (pendrive, disco usb, etc), de acuerdo a lo realizado en el **Método 1**.
· Cable de red (tantos cables como nets se vayan a actualizar) y uno para conectar la máquina de origen con el switch.
· Switch de 8, 16 o 24 bocas que soporte multicast.
· CloneZilla Server portable instalado en un pendrive.
· Habilitado el inicio por **pxe** de las netbooks.
· La net de destino tiene que tener exactamente los mismos detalles físicos y de particiones lógicas a la cual donde se armó la imagen de Huayra. También tiene que tener la opción de inicio por **pxe** habilitado.

Paso 1

En la máquina que se utilizará como netbook madre repetir los pasos del **Método 1** (Instalar la última versión de Huayra, generar la imagen de la partición utilizando CloneZille y reemplazar la imagen de recuperación con esa imagen mediante el script descargado del sitio)

Paso 2

Utilizar el programa GParted (Sistema -> Administración -> GParted) para reconocer el número de la partición para hacer la imagen de CloneZilla:



En la imagen de ejemplo se debe seleccionar la partición **sda1** y **sda5**

Paso 3

Se debe iniciar la maquina actualizada con una versión de CloneZilla para generar una

nueva imagen con ambas particiones a restaurar: la principal con el Sistema Operativo Huayra y la de recuperación que se actualizó mediante el script. Una vez hechas estas imagenes, puede utilizarse cualquier máquina como servidor. Las netbooks **hijas** deben tener la misma estructura de particiones en el disco que la que se utilizó para generar la imagen CloneZilla.

Paso 4

Con la imagen generada de ambas particiones se puede comenzar el proceso de migración masiva.

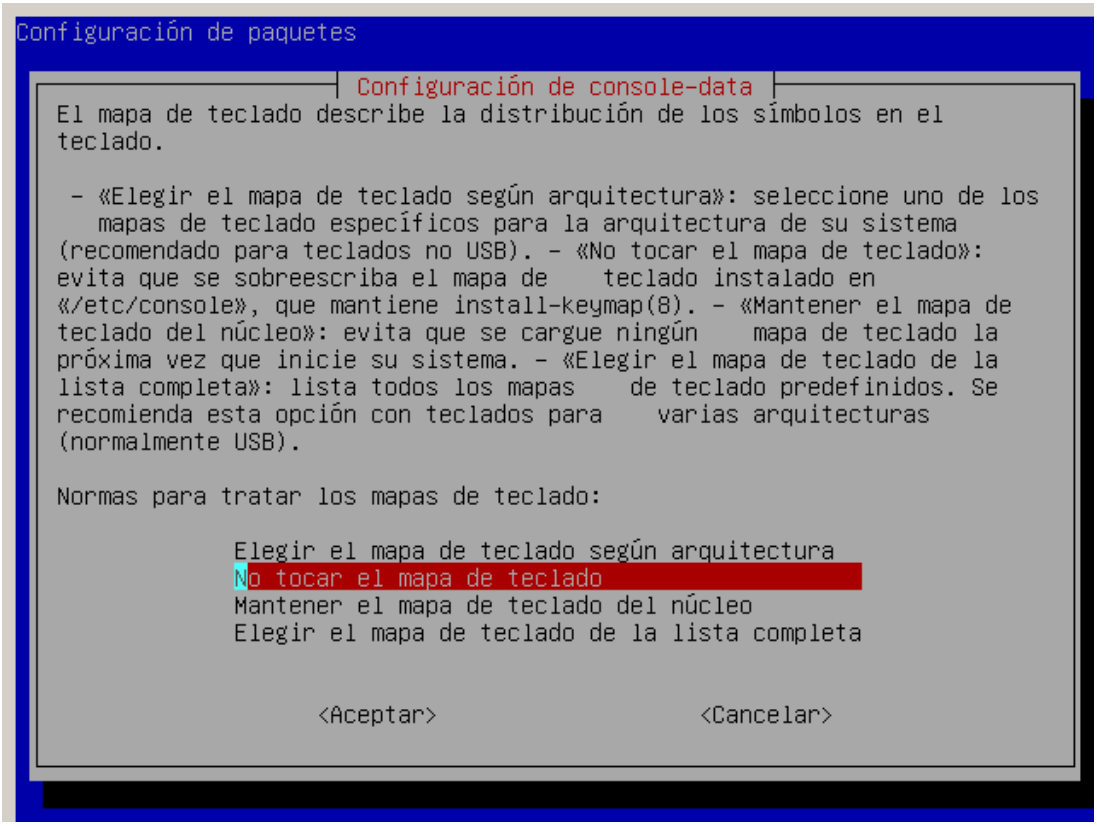
MIGRACIÓN MASIVA

Iniciar la máquina a utilizar como servidor con la imagen del CloneZilla Server. Deberá tener accesible la imagen de las 2 particiones que va a copiar en las máquinas: la de Sistema Operativo Huayra y la de restauración de Huayra.

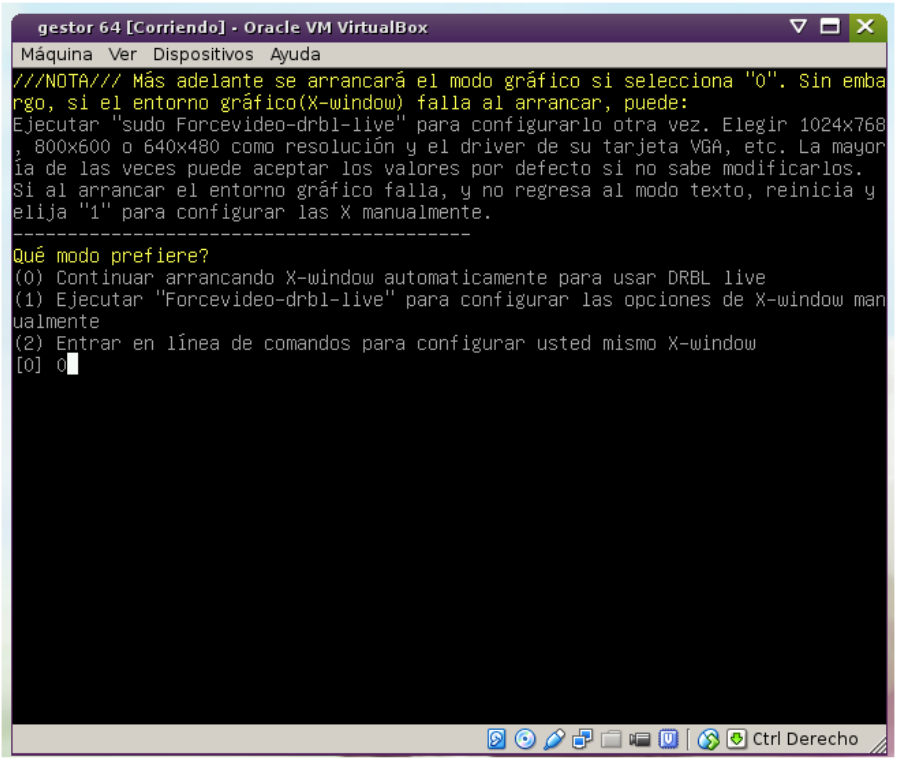
1. Ingresar a la opción **drbl**.

2. Elegir idioma español

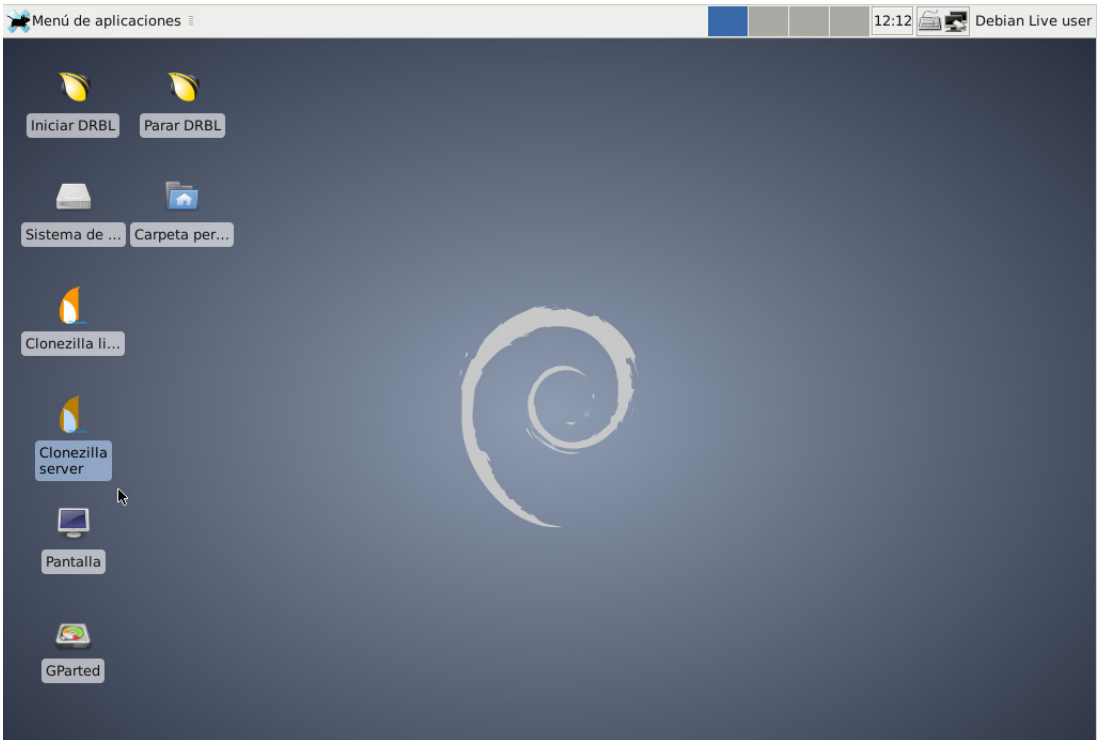
3. No tocar le mapa del teclado



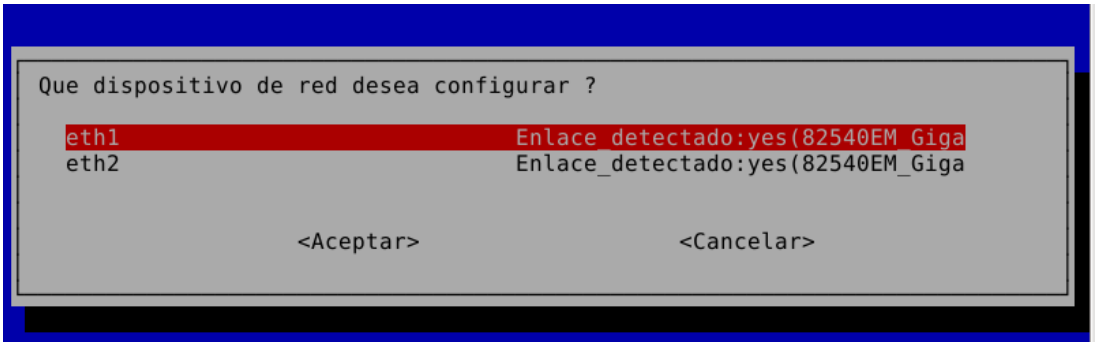
4. Ingresar a la opción DRBL live (0).



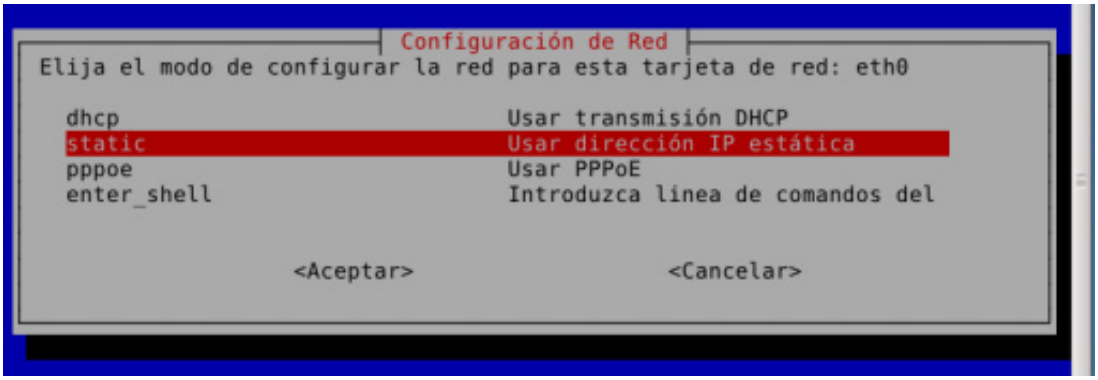
5. Ingresar a la opción clonezilla server.

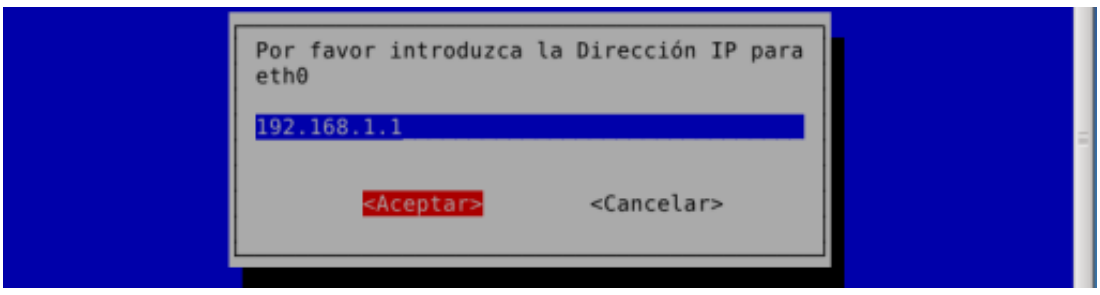


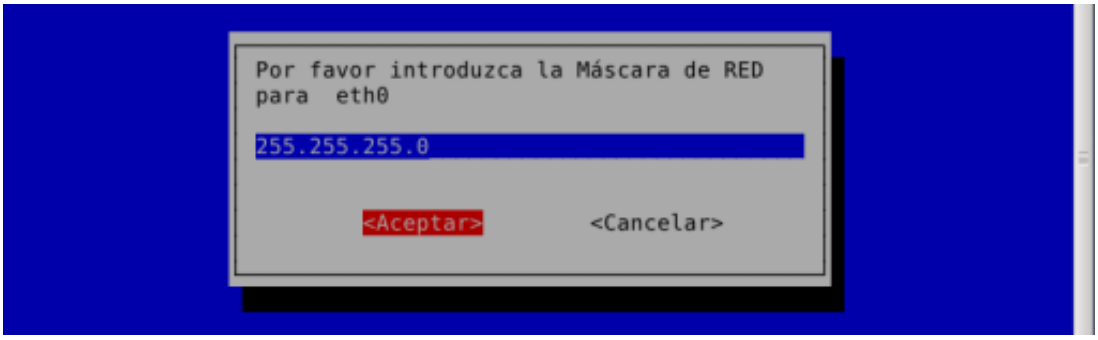
6. Seleccionar la placa de red a utilizar (eth0 / LAN o en caso de no existir eth1).

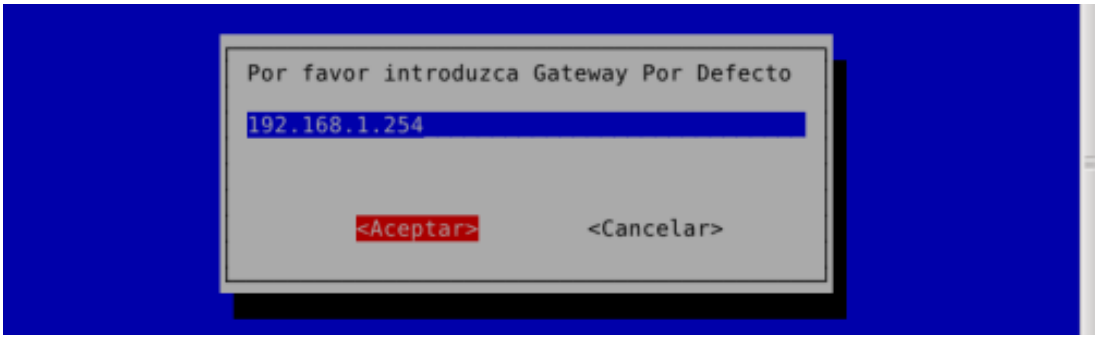


7. IP Estática - Ingresar la IP en el rango existente (por ejemplo 192,168,xxx.x)

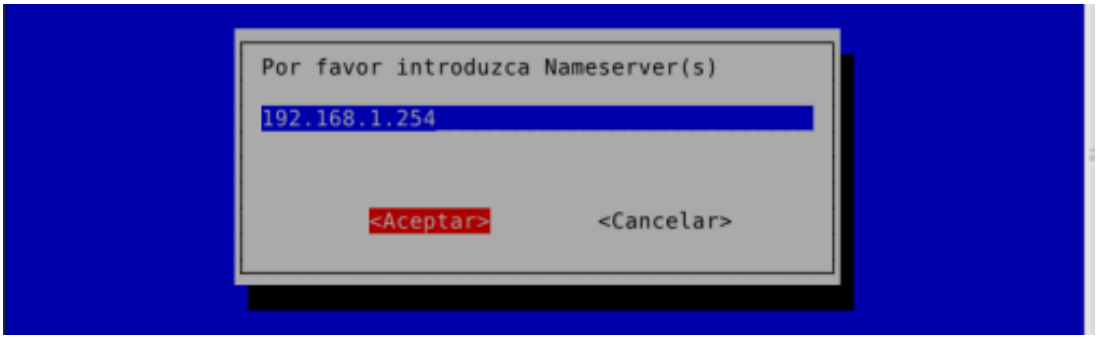


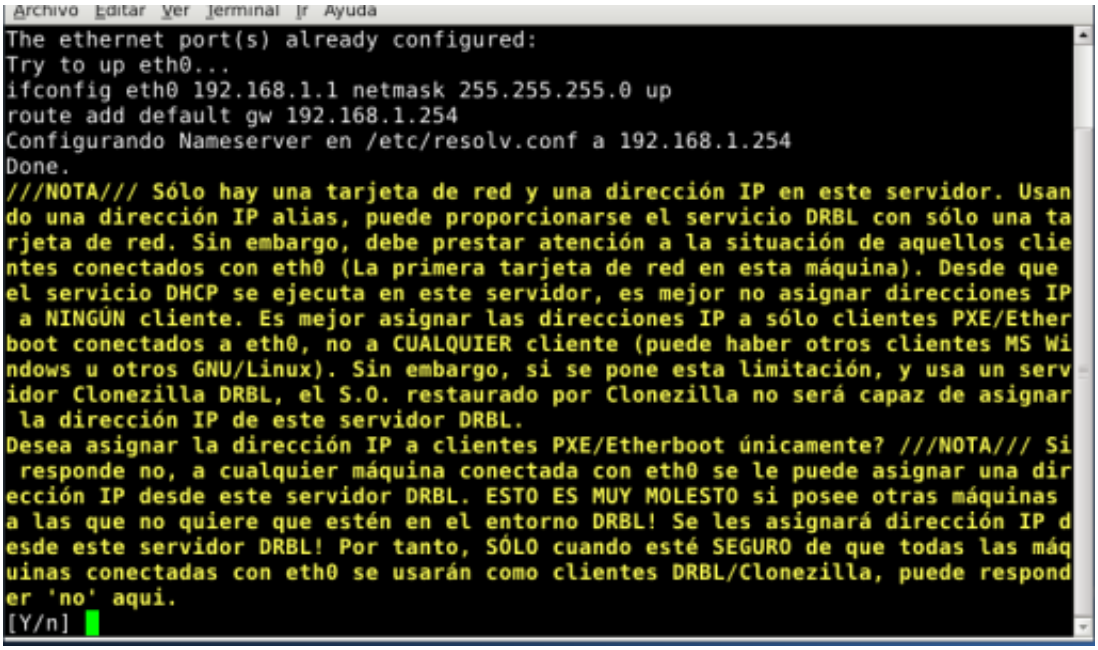






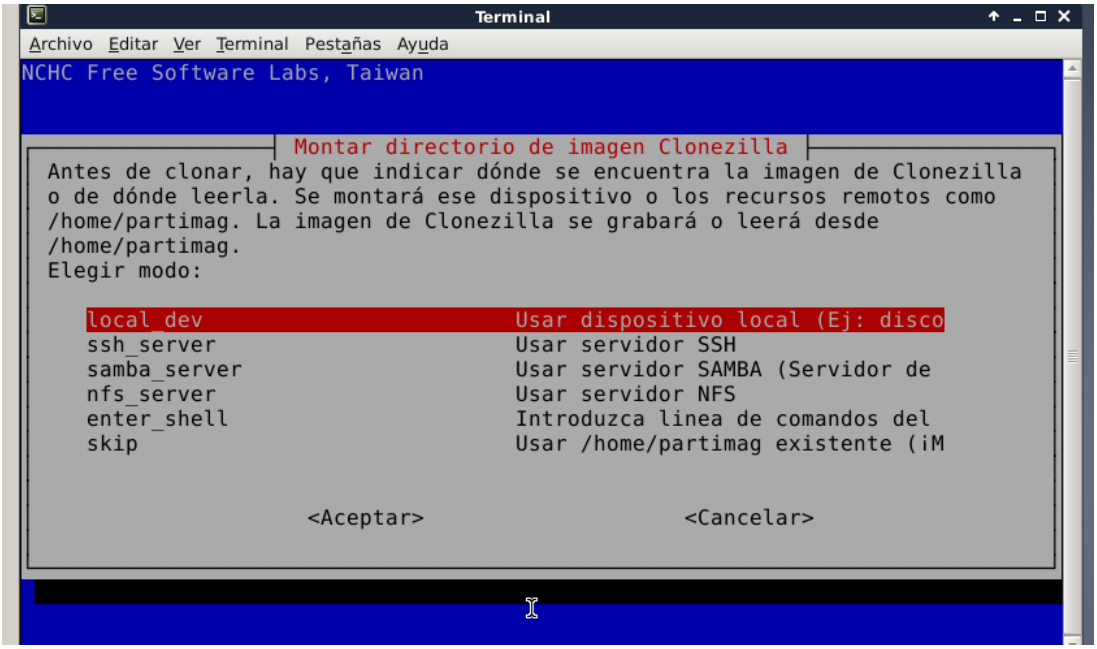
8. Nombre de servidor- IP por defecto.

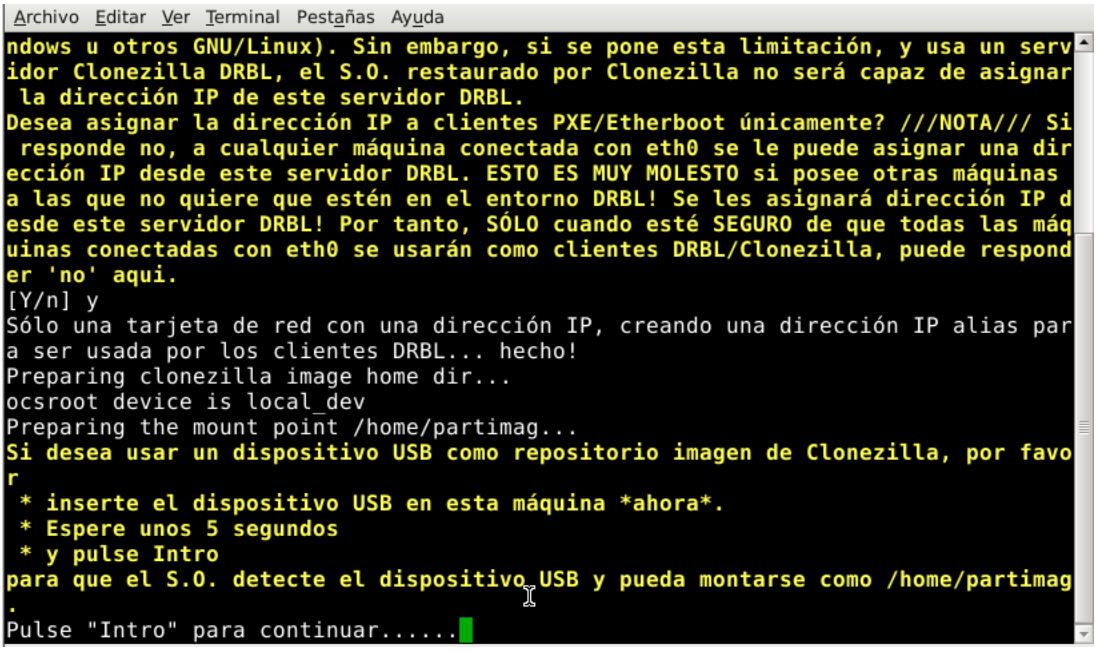




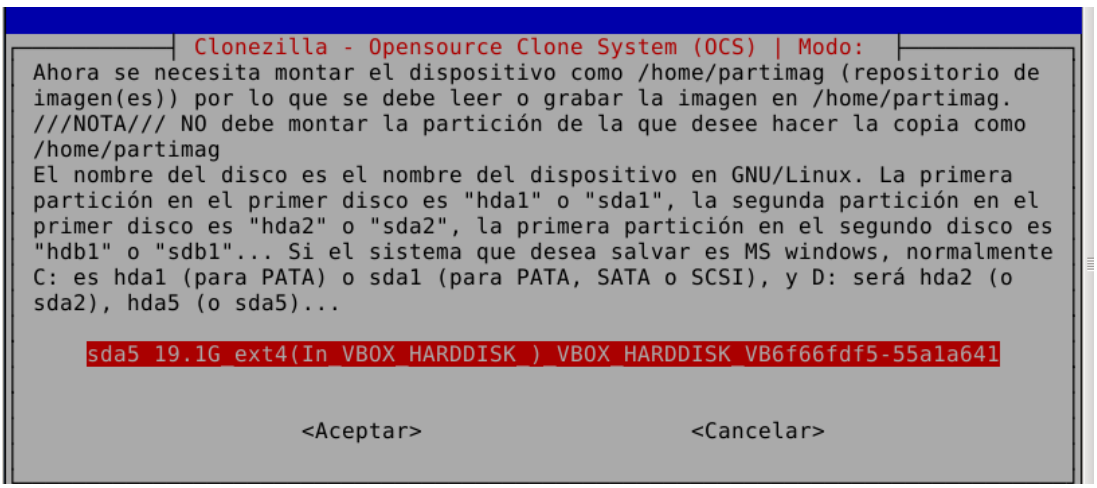
NO CONFIGURAR OTRAS TARJETAS DADO QUE USAREMOS SOLAMENTE LA LAN PARA DHCP / FTP, ETC.

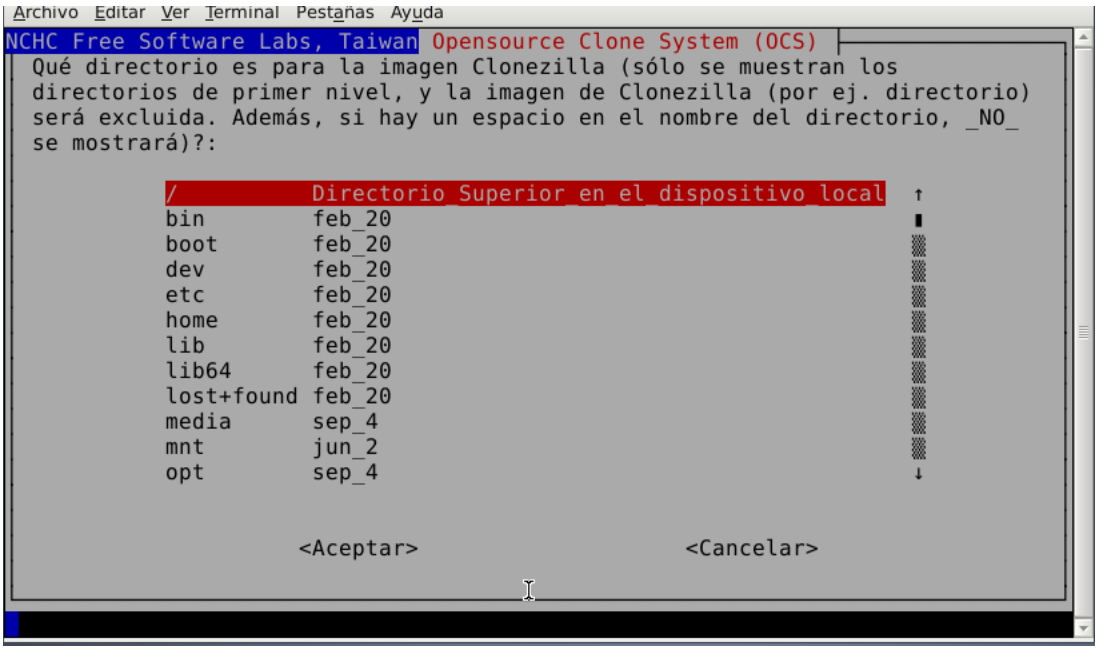
9. Seleccionar tipo de dispositivo donde está la imagen de ambas particiones.

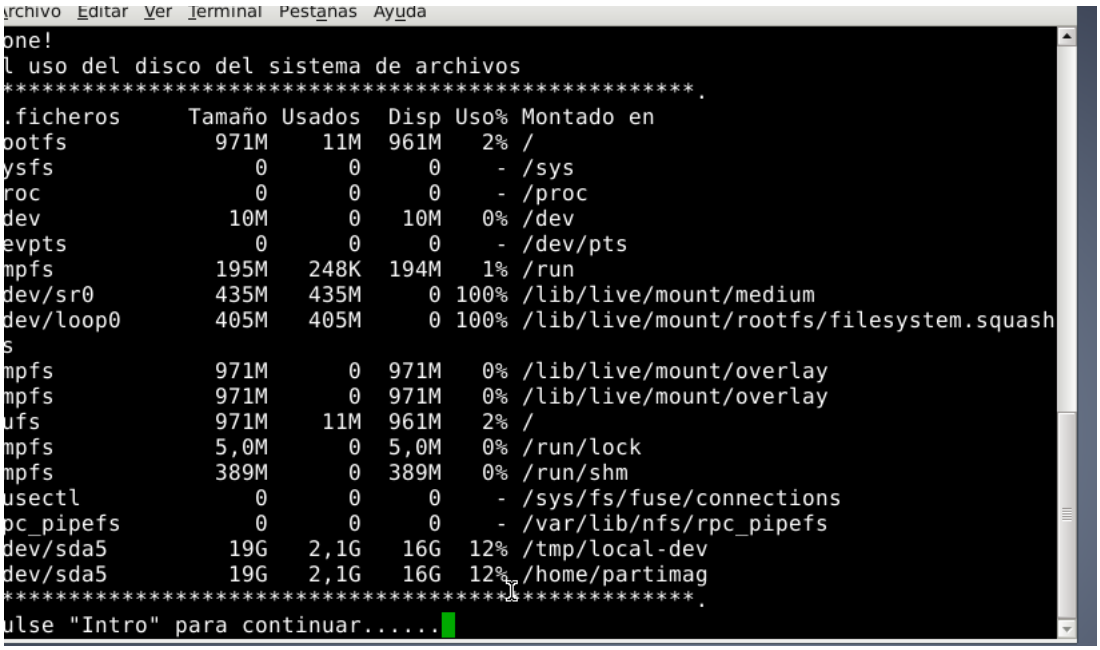




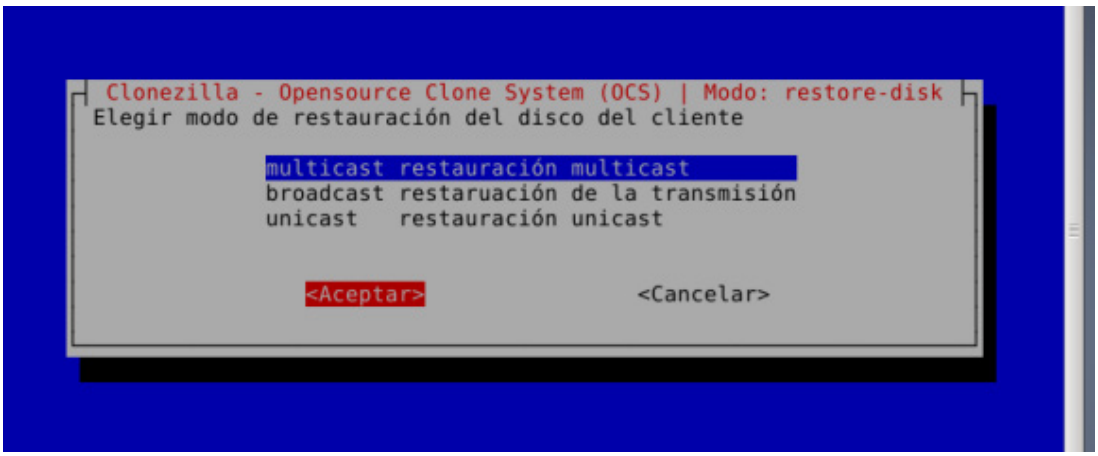
10. Elegir el dispositivo donde se encuentra



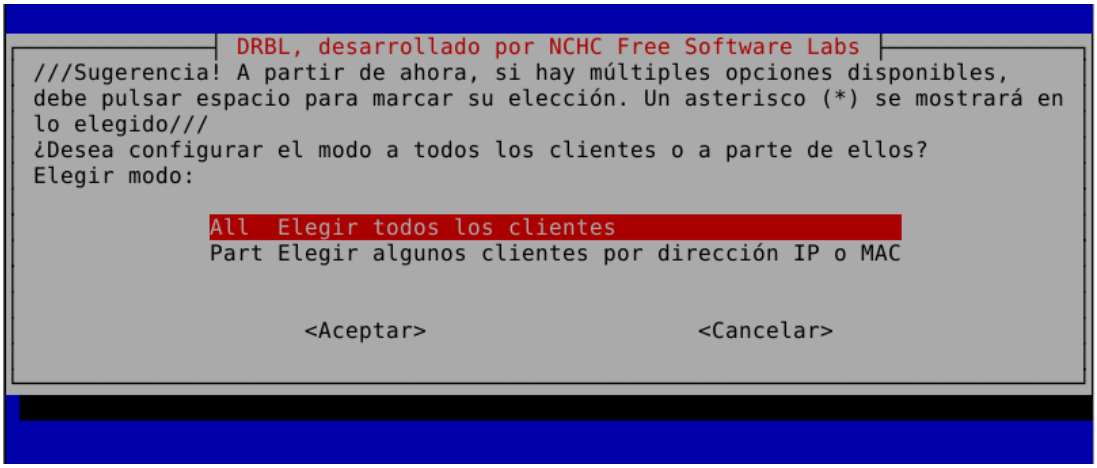




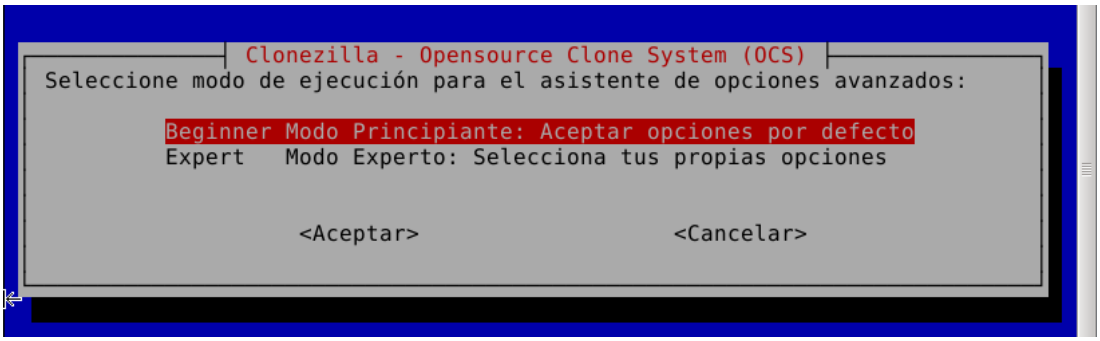
11. Elegir la opción Multicast



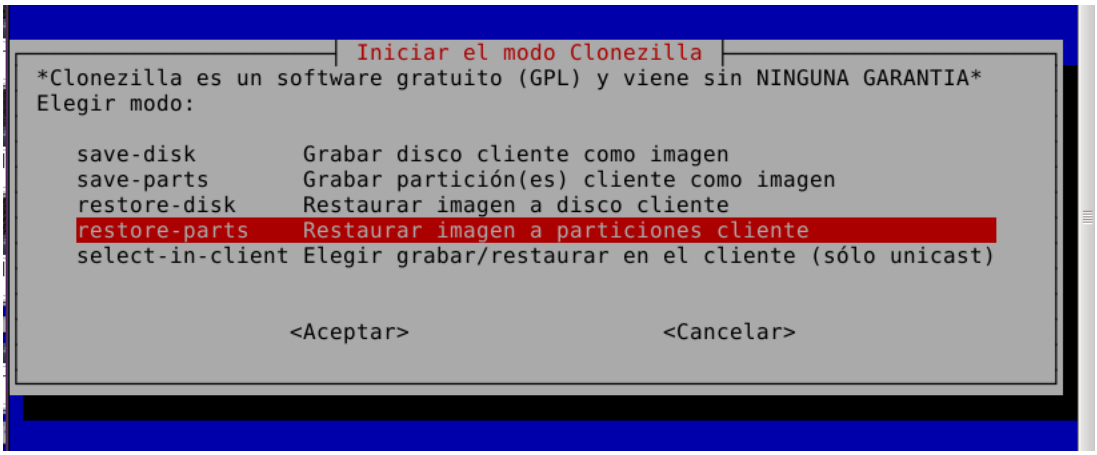
12. Seleccionar la opción **All** Elegir todos los clientes.



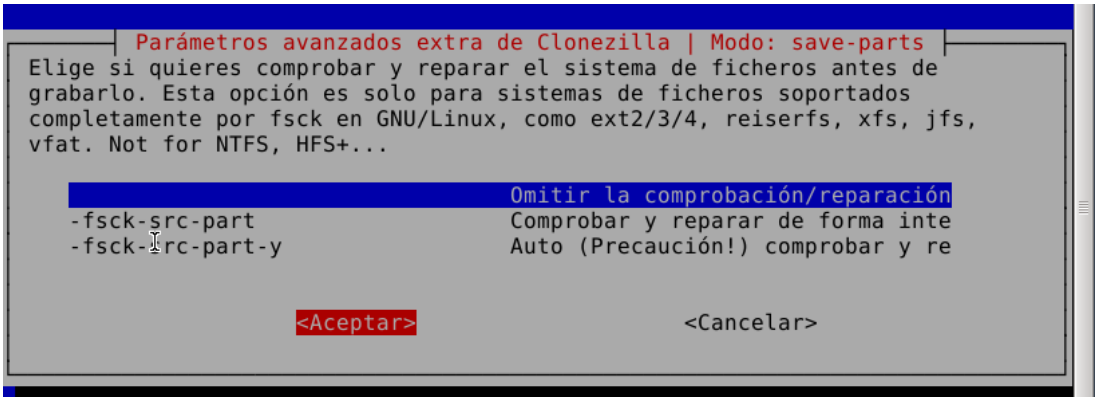
13. Elegir Modo Principiante.



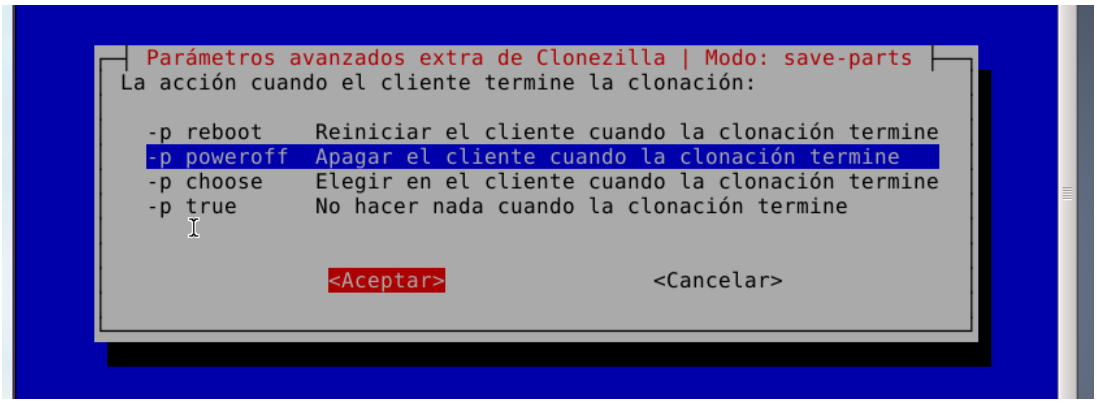
14. Restaurar imagen en particiones clientes.



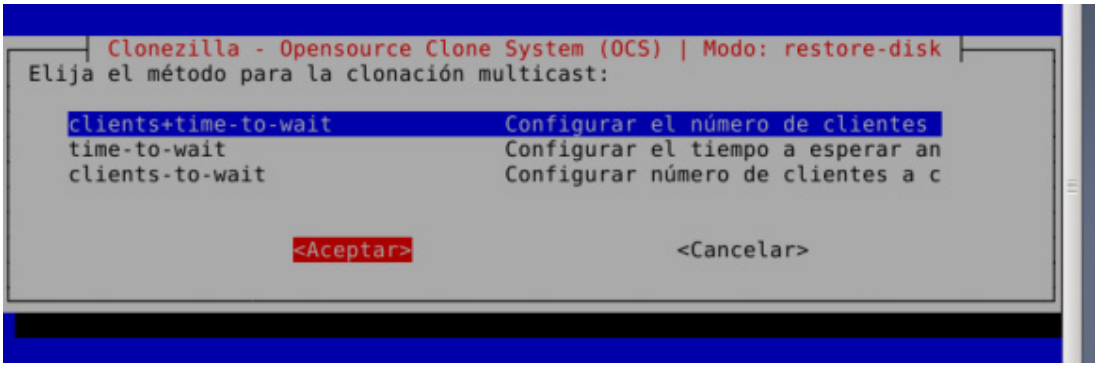
15. Omitir la comprobación de la restauración.



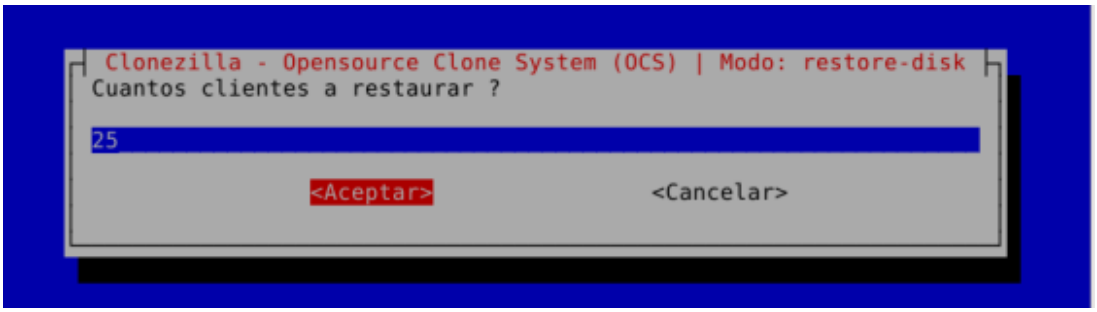
16. Seleccionar que orden se les dará a las maquinas clientes una vez finalizado el proceso.



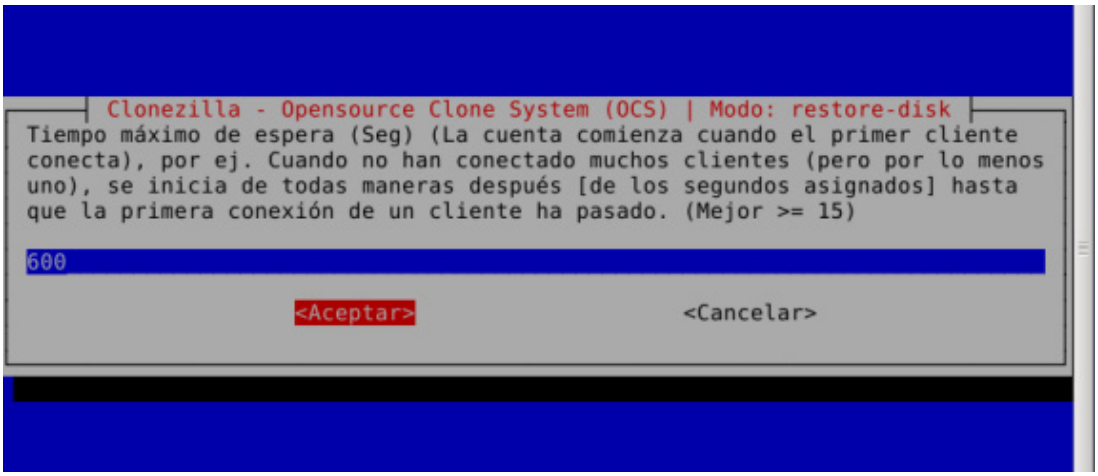
17. Configurar el número de clientes.

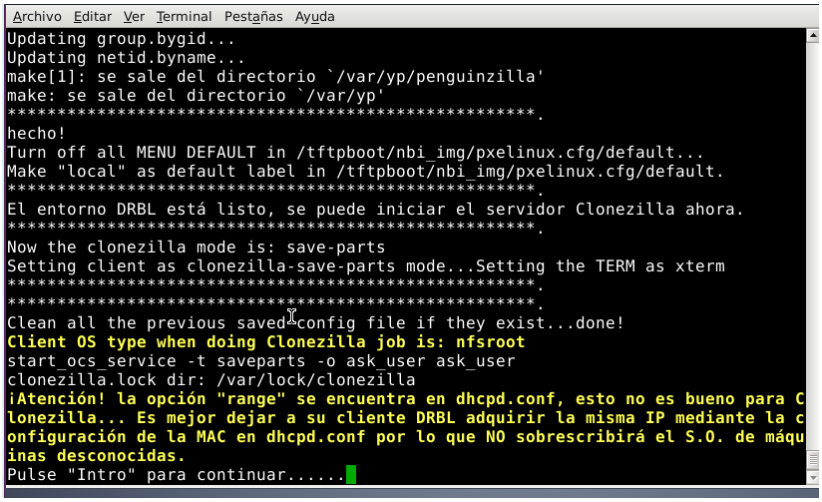


18. Introducir el numero de clientes a restaurar.

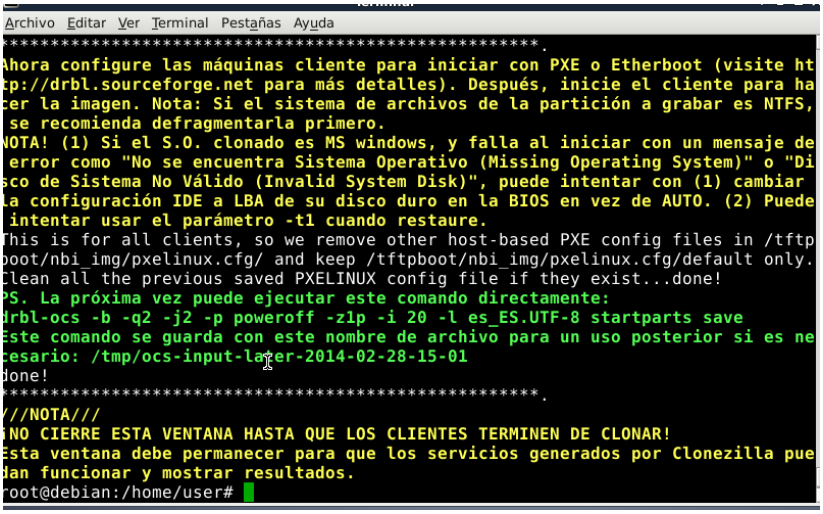


19. Seleccionar el tiempo de espera para el servidor para que inicie la migración.



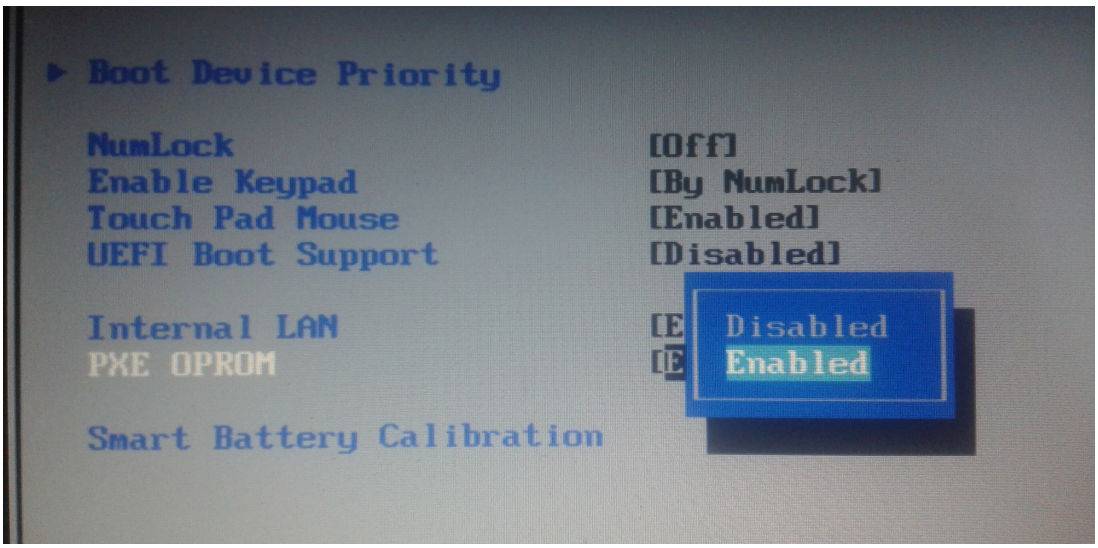


Pantalla de finalización de configuración del DRBL.

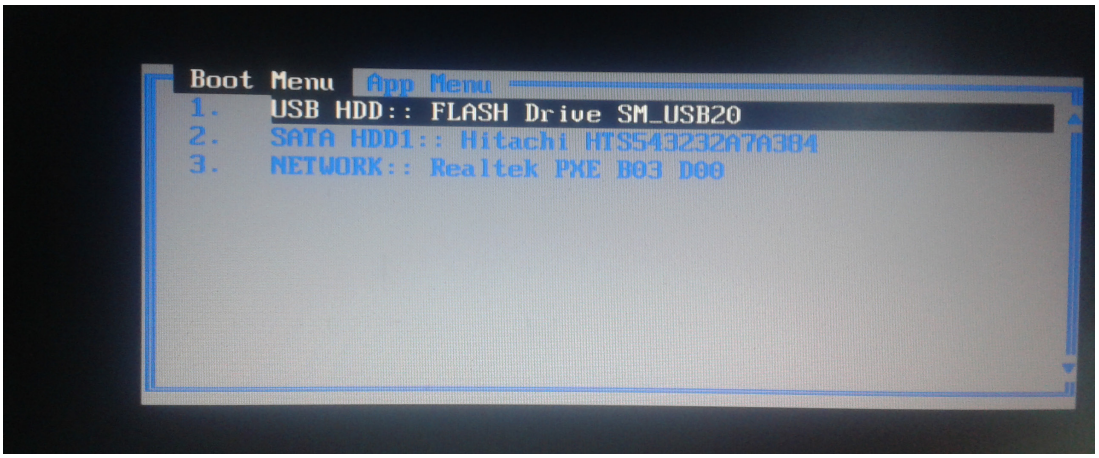


Llegado este punto se deben iniciar las maquinas clientes conectadas al switch con la configuración de PXE en el inicio.

Para hacer esto, ingresar a la Bios y configurar en el menú de Boot la opción PXE (como figura en la siguiente imagen).



Una vez ahí, podemos comprobar que las máquinas están habilitadas a bootear desde PXE si entramos al Boot Menú al encender la máquina (presionando F10, F11 o F12 según el hw que se posea)

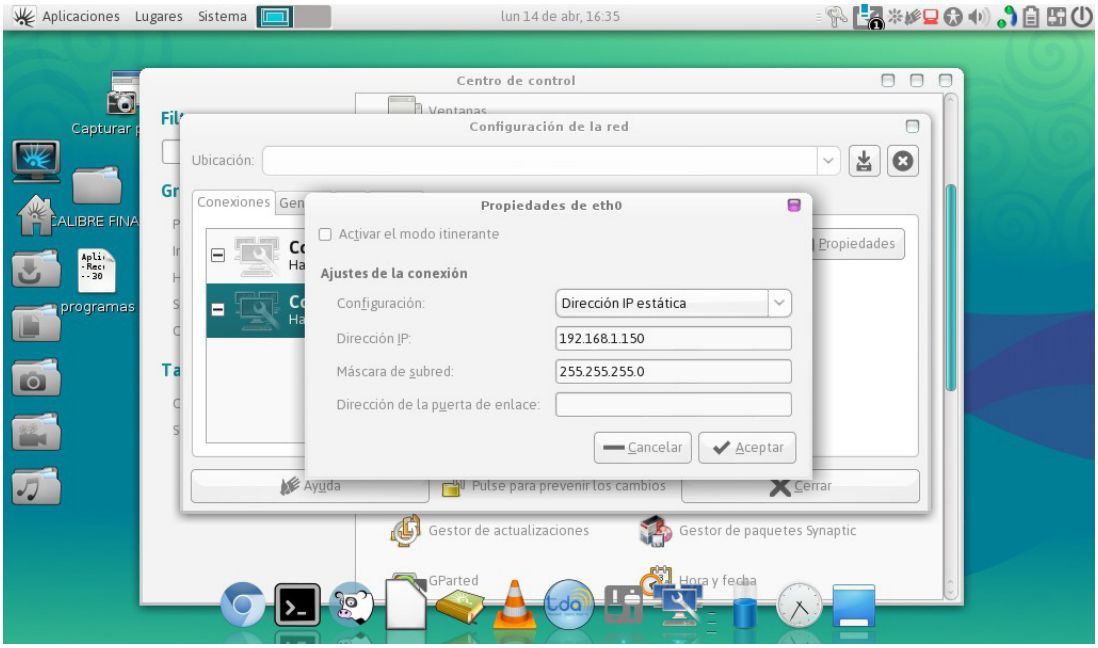


Cuando esto suceda el servidor las actualizara automáticamente cuando finalice el tiempo de espera. No debe tocar las maquinas clientes ni la maquina de origen hasta que no suceda lo que haya seleccionado en la opción previa (apagado, reinicio, etc).

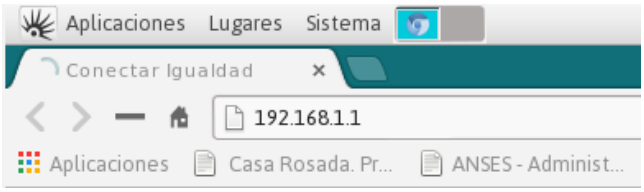
CONFIGURACIÓN ACCESS POINTS
HP V-M200

1) Conectar una Netbook al Access Point HP mediante un cable de red.

2) Cambiar la configuración IP de la Netbook desde **Centro de control / Red**:
   1. IP: 192.168.1.150
   2. Máscara: 255.255.255.0



3) Con el AP HP encendido, ingresar al sitio (mediante un explorador de Internet, este instructivo trabajó con Mozilla Firefox) 192.168.1.1

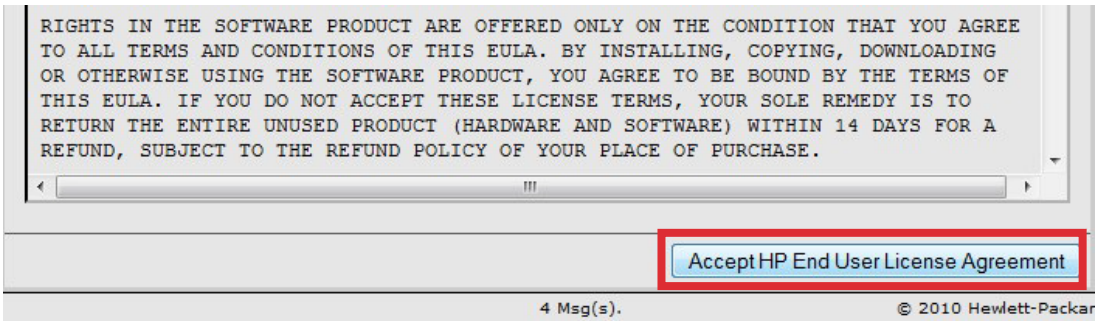


4) Es probable que el navegador de Internet seleccionado presente una advertencia de seguridad. **Haga clic en la opción que permita continuar.**

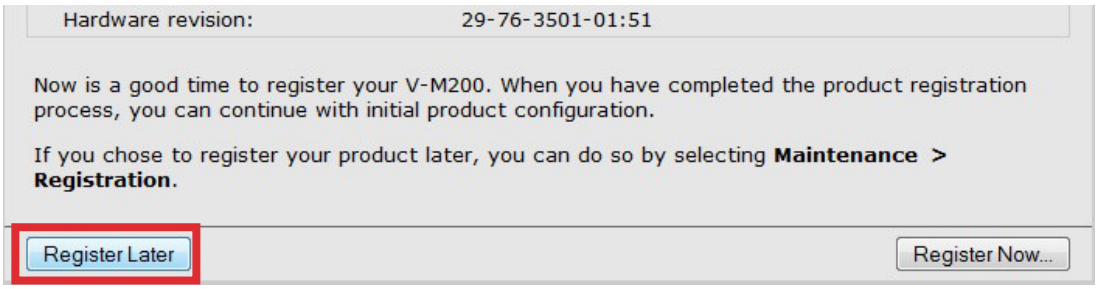
5) Ingresar :

6) Clic en Login.
Username: **admin**
Password: **admin**

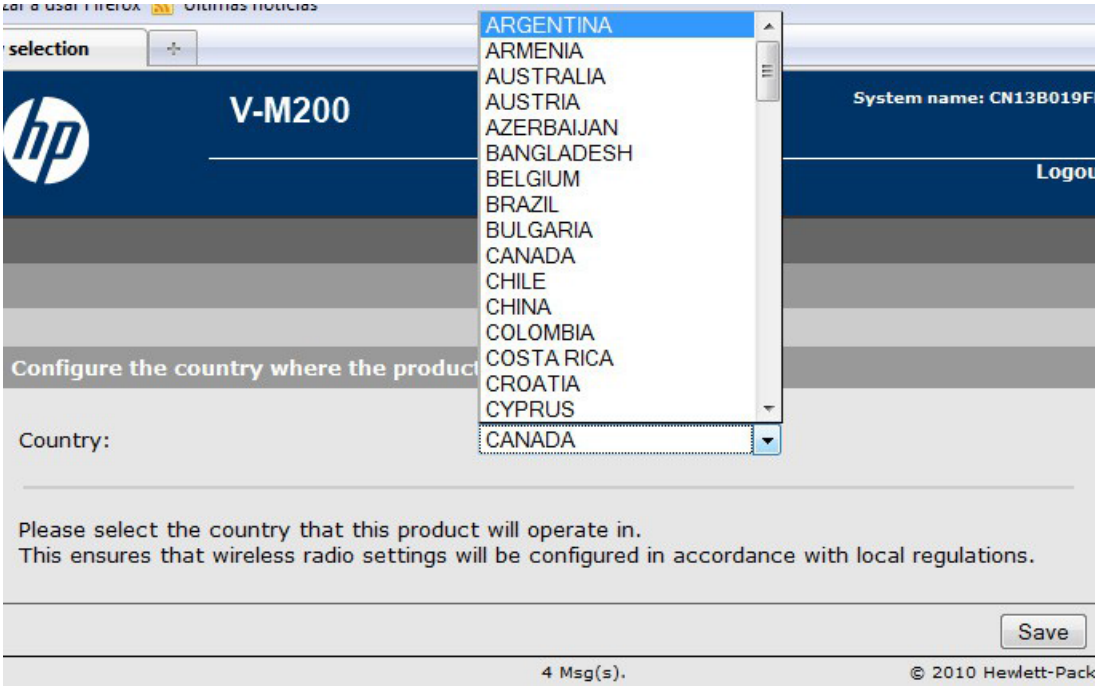
7) Con la barra de desplazamiento del navegador web, ir al final de la página y luego hacer clic sobre **"Accept HP End User License Agreement"**.



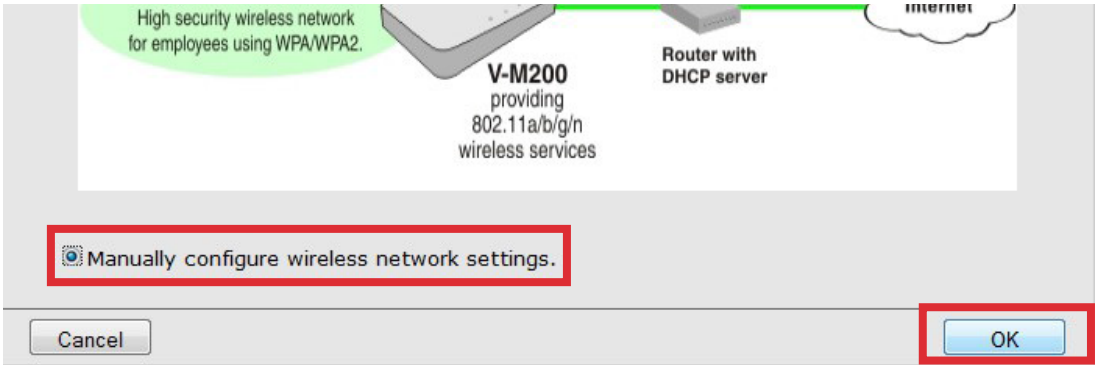
8) Con la barra de desplazamiento del navegador web, ir al final de la página y luego con el botón izquierdo del mouse hacer clic sobre **"Register Later"**.



9) Hacer clic sobre la **selección de países** y luego hacer clic sobre **ARGENTINA**. Luego hacer clic sobre **SAVE**.



10) Con la barra de desplazamiento del navegador web, ir al final de la página y SELECCIONAR **"Manually configure wireless network settings"**, luego nuevamente hacer clic sobre **OK**.



11) Seleccionar la opción **Maintenance**. Luego **"Config file management"**.

12) Bajo **"Restore configuration"**, elija la opción **"Browse"** para navegar hasta el archivo de configuración que se desea restaurar (en los servidores se encuentra en **/home/huayra-admin/Escritorio/Documentos del Administrador/Configuración de AP/HP (Intranet)**).

13) Clic en **RESTORE**.

14) Una vez finalizada la restauración, el AP estará configurado.

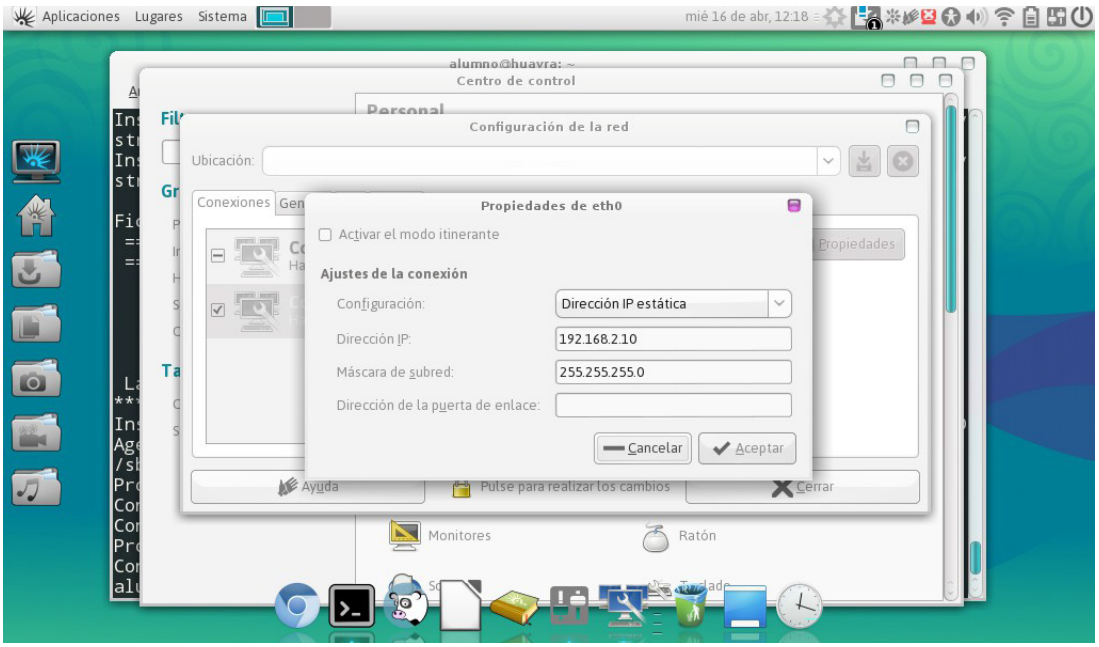
RECUERDE RETIRAR LA CONFIGURACIÓN DE IP DE LA NETBOOK QUE SE UTILIZÓ PARA REALIZAR EL PROCEDIMIENTO.

CONFIGURACIÓN ACCESS POINTS MICRONET

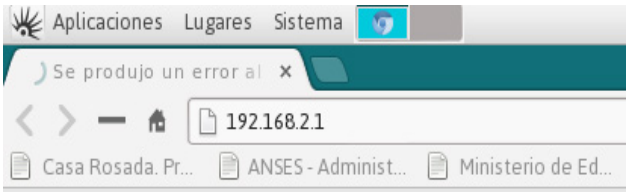
1) Conectar una Netbook al Access Point MICRONET mediante un cable de red.

2) Cambiar la configuración IP de la Netbook desde **Centro de control / Red**:

1. IP: 192.168.2.10
2. Máscara de subred: 255.255.255.0

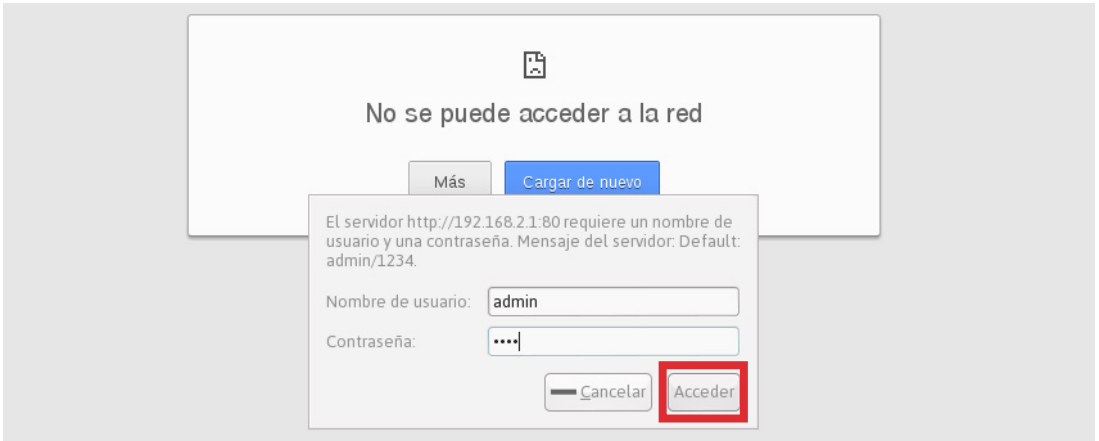


3) Con el AP MICRONET encendido, ingresar al sitio (mediante un explorador de Internet, este instructivo trabajó con Mozilla Firefox) 192.168.2.1



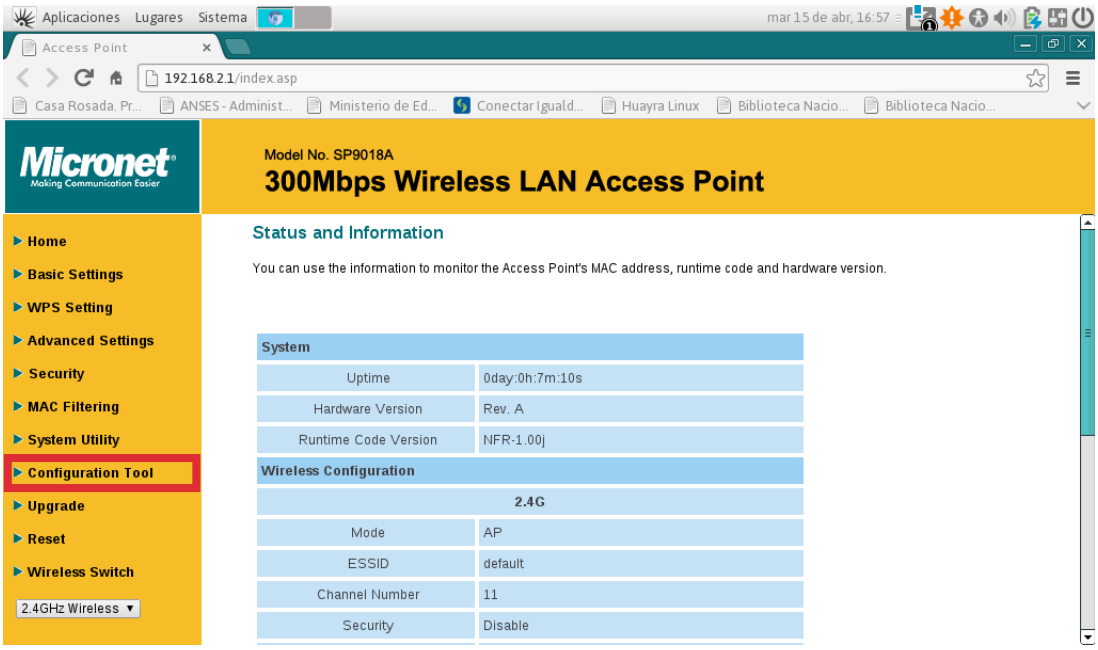
4) Ingresar :

Username: **admin**
Password: **1234**

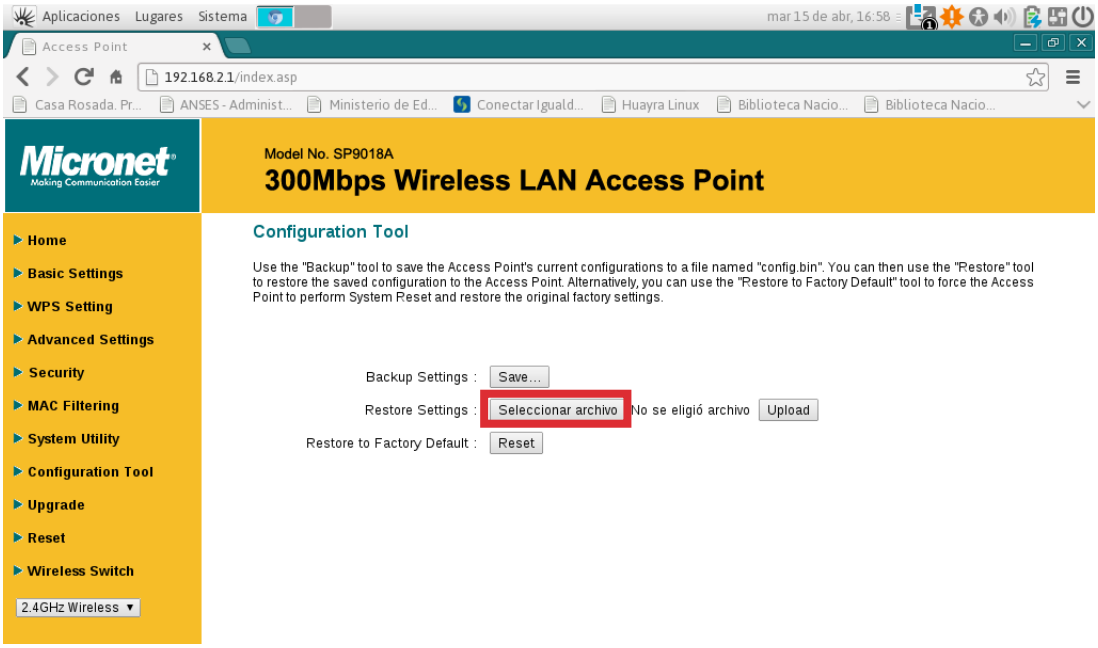


6) Hacer clic en **“Acceder”**.

7) Aparecerá una página de inicio de MICRONET. Allí acceder a **“Configuration Tool”**.



8) En **“Restore Settings”**, hacer clic en **“Seleccionar archivo”**.



9) Allí deberá localizar y seleccionar el archivo de configuración que se encuentra en: **/home/huayra-admin/Escritorio/Documentos del Administrador/Configuración de AP/Micronet (Internet)/CONFIGURACION Micronet.bin**

10) Hacer clic en **UPLOAD**.

11) Finalmente hacer clic en **OK**.

RECUERDE RETIRAR LA CONFIGURACIÓN DE IP DE LA NETBOOK QUE SE UTILIZÓ PARA REALIZAR EL PROCEDIMIENTO.